

SELMER RANKS OF TWISTS OF HYPERELLIPTIC CURVES AND SUPERELLIPTIC CURVES*

MYUNGJUN YU

ABSTRACT. We study the variation of Selmer ranks of Jacobians of twists of hyperelliptic curves and superelliptic curves. We find sufficient conditions for such curves to have infinitely many twists whose Jacobians have Selmer ranks equal to r , for any given nonnegative integer r . This generalizes earlier results of Mazur-Rubin on elliptic curves.

INTRODUCTION

Let E be an elliptic curve over \mathbf{Q} . Goldfeld's conjecture predicts that 50% of elliptic curves have rank 0 and 50% have rank 1 in the family of quadratic twists of E . Let E^χ denote the quadratic twist of E by a quadratic character χ . We write $\text{Sel}_2(E/\mathbf{Q})$ and $\text{III}_{E/\mathbf{Q}}$ to denote the 2-Selmer group and the Shafarevich-Tate group of E/\mathbf{Q} , respectively. Then the following sequence is exact for all χ :

$$0 \rightarrow E^\chi(\mathbf{Q})/2E^\chi(\mathbf{Q}) \rightarrow \text{Sel}_2(E^\chi/\mathbf{Q}) \rightarrow \text{III}_{E^\chi/\mathbf{Q}}[2] \rightarrow 0.$$

Thereby we deduce that

$$\dim_{\mathbf{F}_2}(\text{Sel}_2(E^\chi/\mathbf{Q})) = \text{rk}(E^\chi(\mathbf{Q})) + \dim_{\mathbf{F}_2}(E^\chi(\mathbf{Q})[2]) + \dim_{\mathbf{F}_2}(\text{III}_{E^\chi/\mathbf{Q}}[2]),$$

where $\text{rk}(E^\chi(\mathbf{Q}))$ is the Mordell-Weil rank (over \mathbf{Q}) of E^χ . If we assume the Shafarevich-Tate Conjecture along with Goldfeld's conjecture, so $\dim_{\mathbf{F}_2}(\text{III}_{E^\chi/\mathbf{Q}}[2])$ is even by Cassels' pairing, we have (varying χ)

- (1)
 - 50% of E^χ have even 2-Selmer ranks and
 - 50% of E^χ have odd 2-Selmer ranks

in the family of quadratic twists of E/\mathbf{Q} , since $\dim_{\mathbf{F}_2}(E^\chi(\mathbf{Q})[2])$ are the same for all χ . This turns out to be true even if we assume neither of those big conjectures (see [4, Corollary 7.10]).

Let $C_{2,f}/\mathbf{Q}$ be a hyperelliptic curve whose affine model is

$$y^2 = f(x),$$

where f is a (separable) polynomial defined over \mathbf{Q} , and $\deg(f)$ is odd. Then it is interesting to know if we can show that (1) holds when E is replaced by the Jacobian of $C_{2,f}$ (denoted by J). In other words, is it true that

- (2)
 - 50% of J^χ have even 2-Selmer ranks, and
 - 50% of J^χ have odd 2-Selmer ranks

in the family of quadratic twists of J/\mathbf{Q} ? It turns out to be true if $\deg(f) \equiv 3 \pmod{4}$, and false if $\deg(f) \equiv 1 \pmod{4}$ (see Corollary 7.6, Proposition 8.1, and

*This material is based upon work supported by the National Science Foundation under grant DMS-1065904.

Proposition 8.4). It is even possible that $\dim_{\mathbf{F}_2}(\text{Sel}_2(J^\chi/\mathbf{Q}))$ has constant parity for all χ when $\deg(f) \equiv 1 \pmod{4}$. We display such examples in Section 8. In fact, we prove (Theorem 7.4):

Theorem 1. *For all sufficiently large X ,*

$$\frac{|\{\chi \in \mathcal{C}(K, X) : d_2(\text{Sel}_2(J^\chi/K)) \text{ is even}\}|}{|\mathcal{C}(K, X)|} = \frac{1 + \delta}{2},$$

where $\mathcal{C}(K, X)$ and δ are defined in Definition 7.2 and Definition 7.1, respectively.

This theorem generalizes an earlier result of Klagsbrun, Mazur, and Rubin on elliptic curves ([4, Theorem 7.6]) to Jacobians of hyperelliptic curves.

Aside from the parity distribution, two questions we could ask for the family of quadratic twists of J over a number field K are, “how many integers does the set $A_J := \{\dim_{\mathbf{F}_2}(\text{Sel}_2(J^\chi/K)) \mid \chi \text{ is a quadratic character}\}$ cover,” and, “under what conditions does $A_J = \mathbf{Z}_{\geq 0}$ happen?” This question was inspired by Mazur-Rubin’s work ([8, Theorem 1.6]) on elliptic curves as follows:

Theorem 2. [8, Theorem 1.6] *Suppose that K is a number field, and E is an elliptic curve over K such that $\text{Gal}(K(E[2])/K) \cong S_3$. Let Δ_E be the discriminant of some model of E , and suppose further that K has a place v_0 satisfying one of the following conditions:*

- v_0 is real and $(\Delta_E)_{v_0} < 0$, or
- $v_0 \nmid 2\infty$, E has multiplicative reduction at v_0 , and $\text{ord}_{v_0}(\Delta_E)$ is odd.

Then for every $r \geq 0$, there are infinitely many quadratic twists E'/K of E such that $\dim_{\mathbf{F}_2}(\text{Sel}_2(E'/K)) = r$.

We study the generalization of Theorem 2 to Jacobians of hyperelliptic and superelliptic curves in this paper. We write $C_{p,f}$ to denote the superelliptic curve (Definition 1.1), which is the smooth projective curve whose affine model is given by $y^p = f(x)$, where $f(x)$ is a separable polynomial of degree ≥ 2 . In particular, when $p = 2$, we call $C_{2,f}$ a hyperelliptic curve. We denote the Jacobian of a (smooth projective) curve C by $J(C)$. We prove (Corollary 7.9):

Theorem 3. *Suppose that K is a number field and $f \in K[x]$ is a separable polynomial. Let $n = \deg(f)$ and suppose that $n \equiv 3 \pmod{4}$ and $\text{Gal}(f) \cong S_n$ or A_n . Suppose further that K has a real embedding. Then for every $r \geq 0$, the Jacobian J of $C_{2,f}$ has infinitely many quadratic twists J^χ such that $\dim_{\mathbf{F}_2}(\text{Sel}_2(J^\chi/K)) = r$.*

Our technique relies on the fact that there is a canonical G_K -module isomorphism between $J(C_{2,f})[2]$ and $J(C_{2,df})[2]$, so that we can compare two Selmer groups

$$\text{Sel}_2(J(C_{2,f})/K) \subset H^1(K, J(C_{2,f})[2]) \text{ and}$$

$$\text{Sel}_2(J(C_{2,df})/K) \subset H^1(K, J(C_{2,df})[2]) \cong H^1(K, J(C_{2,f})[2])$$

in $H^1(K, J(C_{2,f})[2])$. We work more generally with π -Selmer groups ($\pi := 1 - \zeta_p$, where ζ_p is a primitive p -th root of unity) of superelliptic curves $C_{p,f}$ for arbitrary prime numbers p . Note that if $p = 2$, then $\pi = 1 - \zeta_2 = 2$, so π -Selmer group (which will be defined in Section 3) is actually a 2-Selmer group of a hyperelliptic curve $C_{2,f}$ in this case. As in the hyperelliptic curve case, it is essential to compare $\text{Sel}_\pi(J(C_{p,f})/K)$ and $\text{Sel}_\pi(J(C_{p,df})/K)$ in $H^1(K, J(C_{p,f})[\pi])$, which is possible because there is a G_K -module isomorphism between $J(C_{p,f})[\pi]$ and $J(C_{p,df})[\pi]$ as will

be seen in Proposition 1.7. We get a similar result when $p \geq 3$, as follows (Theorem 4.13).

Theorem 4. *Suppose that K is a number field containing ζ_p , and $f \in K[x]$ is a separable polynomial. Let $n = \deg(f)$ and suppose that $p \nmid n$ is an odd prime and $\text{Gal}(f) \cong S_n$. Then for every $r \geq 0$, the superelliptic curve $C_{p,f}$ has infinitely many p -twists $C_{p,df}$ where $d \in K^\times / (K^\times)^p$ such that $\dim_{\mathbf{F}_p}(\text{Sel}_\pi(J(C_{p,df})/K)) = r$.*

In the elliptic curve case, Kramer showed that (see [5, Theorem 1] and [8, Theorem 2.8]) there is a (parity) relation between two Selmer groups $\text{Sel}_2(E/K)$ and $\text{Sel}_2(E^\chi/K)$ as follows:

$$\dim_{\mathbf{F}_2}(\text{Sel}_2(E/K)) - \dim_{\mathbf{F}_2}(\text{Sel}_2(E^\chi/K)) \equiv \sum_v h_v(\chi_v) \pmod{2},$$

where χ_v is the restriction of χ to G_{K_v} , and $h_v(\chi_v)$ is defined locally for every place v (Definition 2.2). In this paper, with the aid of [4, Theorem 3.9] we extend this result to Jacobians of hyperelliptic curves (Theorem 5.11). In fact, this generalization plays an important role in proving Theorem 1.

We briefly sketch the main idea of the proofs of Theorem 3 and Theorem 4 here. Since a Selmer group is determined by its local conditions, if we find an element $d \in K^\times / (K^\times)^p$ such that local conditions defining $\text{Sel}_\pi(J(C_{p,f})/K)$ and $\text{Sel}_\pi(J(C_{p,df})/K)$ are the same everywhere except at only one place v , then we may expect $\text{Sel}_\pi(J(C_{p,f})/K)$ and $\text{Sel}_\pi(J(C_{p,df})/K)$ are “almost” the same. By choosing an appropriate d , we increase or decrease the π -Selmer ranks by 1 under the assumptions of Theorem 4. But in the hyperelliptic curve case, it turns out it is difficult to increase or decrease 2-Selmer ranks by 1 by twisting only with this idea. But under sufficiently good conditions (see Theorem 6.7), it is possible to increase or decrease 2-Selmer ranks by 2 by twisting. To prove this, we use the structure of metabolic spaces and the quadratic forms arising from the Heisenberg groups. Then with the aid of Theorem 1, we prove Theorem 3.

The layout of the paper is as follows. In Section 1, we define a p -twist J^χ of the Jacobian J of a superelliptic curve $C_{p,f}$. In Section 2, we assume $C_{p,f}$ is defined over a local field K_v . We compare local conditions (the Kummer images arising from $\pi : J \rightarrow J$, and $\pi : J^\chi \rightarrow J^\chi$), which are in fact the defining local conditions of π -Selmer groups of J and J^χ . In Section 3, we define various Selmer groups. In Section 4, Theorem 4 will be proved. Section 5 defines the quadratic form arising from Heisenberg group that we will need in the sequel. Section 6 and Section 7 will be devoted to prove Theorem 1 and Theorem 3, which shows that (2) is true if $\deg(f) \equiv 3 \pmod{4}$. Section 8 contains an explicit example of the Jacobian of $C_{2,f}$ ($\deg(f) \equiv 1 \pmod{4}$), whose quadratic twists have constant 2-Selmer rank parity, so (2) is not satisfied.

1. SUPERELLIPTIC CURVES AND TWISTS

In this section, we fix a prime p and a field L containing ζ_p , where ζ_p is a primitive p -th root of unity. We assume that L has characteristic 0. Consider a plane curve

$$S : y^p = f(x),$$

where f is a separable polynomial over L . If $p \nmid \deg(f)$, then S is normalized to a smooth projective curve, with one rational point at infinity that we will denote

by ∞ . See [17, §1] for the justification. Note that this holds for all f such that $p \nmid \deg(f)$ although [17] treats only the case when $\deg(f) > p$ for another reason.

Definition 1.1. A superelliptic curve $C_{p,f}$ over L is a smooth projective curve in the projective space \mathbb{P}^2 whose affine model is

$$y^p = f(x),$$

where f is a separable polynomial (not necessarily monic) defined over K such that $p \nmid \deg(f)$. When $p = 2$, we call it a hyperelliptic curve.

Suppose that $\alpha_1, \alpha_2, \dots, \alpha_n$ are the roots of f , where n denotes the degree of f . For every smooth projective curve C , let $J(C)$ denote the Jacobian of C . Then $J(C_{p,f})$ is generated by divisor classes of the form $[P - \infty]$, where P is a point of $y^p = f(x)$.

Fix a primitive p -th root of unity ζ_p , and let $\pi := 1 - \zeta_p$. Then we have $\pi^{p-1} = pu$ for a unit $u \in \mathbf{Z}[\zeta_p]$. We often write J instead of $J(C_{p,f})$ when it is obvious in the context.

Remark 1.2. Let $C_{p,f}$ be a superelliptic curve defined over L of characteristic 0. Note that $J(C_{p,f})$ has a natural $\mathbf{Z}[\zeta_p]$ -action induced by $\zeta_p(\alpha, \beta) = (\alpha, \zeta_p \beta)$, where (α, β) is a point of $y^p = f(x)$. In other words, there is a natural map

$$\mu_p \rightarrow \text{Aut}(J(C_{p,f})),$$

where μ_p is the multiplicative group of p -th roots of unity. Let $\alpha_1, \alpha_2, \dots, \alpha_n$ be the roots of $f(x)$. Then

$$[(\alpha_1, 0) - \infty], [(\alpha_2, 0) - \infty], \dots, [(\alpha_{n-1}, 0) - \infty]$$

form a basis of $J[\pi]$ by [15, Proposition 3.2], where $J[\pi]$ denotes the \mathbf{F}_p -vector space of the π -torsion points of $J(C_{p,f})$. Note that

$$[(\alpha_n, 0) - \infty] = -[(\alpha_1, 0) - \infty] - [(\alpha_2, 0) - \infty] - \dots - [(\alpha_{n-1}, 0) - \infty].$$

Remark 1.3. The symmetric group S_n naturally acts on the set of the roots of f . This induces an action of S_n on $J[\pi]$. Note that $\text{Gal}(f) \subset S_n$ acts on $J[\pi]$ naturally too.

Definition 1.4. Let L be a field of characteristic 0, and $\zeta_p \in L$. We write

$$\mathcal{C}^p(L) := \text{Hom}(G_L, \mu_p).$$

If L is a local field, we often identify $\mathcal{C}^p(L)$ with $\text{Hom}(L^\times, \mu_p)$ via the local reciprocity map, and let $\mathcal{C}_{\text{ram}}^p(L) \subset \mathcal{C}^p(L)$ be the subgroup of ramified characters in $\mathcal{C}^p(L)$. Then $\chi \in \mathcal{C}_{\text{ram}}^p(L)$ if and only if $\chi(\mathcal{O}_L^\times) \neq 1$, where \mathcal{O}_L^\times is the unit group of the integer ring of L , by local class field theory.

Definition 1.5. For $\chi \in \mathcal{C}^p(L)$, we say that J^χ is the p -twist of J by χ if J^χ is a superelliptic curve whose affine model is

$$y^2 = d^{-1}f(x),$$

where d is the preimage of χ in the Kummer map

$$L^\times / (L^\times)^p \cong \text{Hom}(G_L, \mu_p);$$

i.e., $J^\chi = J(C_{p,d^{-1}f})$.

Remark 1.6. For any superelliptic curve $C_{p,f}$ defined over K of characteristic 0, an isomorphism over \overline{K} between two affine curves

$$\{y^p = d^{-1}f(x)\} \cong \{y^p = f(x)\}$$

is given by sending (a, b) to $(a, \sqrt[p]{db})$ where $\sqrt[p]{d}$ is a choice of p -th root of d . The following proposition is an immediate consequence of Remark 1.2.

Proposition 1.7. *Suppose that a superelliptic curve $C_{p,f}$ is defined over a field L of characteristic 0, and $\chi \in \mathcal{C}^p(L)$. Then*

$$J[\pi] \cong J^\chi[\pi].$$

In particular, $J(L)[\pi] \cong J^\chi(L)[\pi]$.

Remark 1.8. Let J/L be the Jacobian of a superelliptic curve $C_{p,f}$. We denote the set of twists of J/L by $\text{Twist}(J/L)$. It is well-known (for example, see Proposition 5 in [16, Chapter3 §1]) that there is a bijection

$$\text{Twist}(J/L) \rightarrow H^1(G_L, \text{Aut}(J)).$$

It maps $\phi : A' \rightarrow J$ to $\xi : G_L \rightarrow \text{Aut}(J)$, where $\xi_\sigma = \phi^\sigma \circ \phi^{-1}$.

Then we have a composition of maps

$$(3) \quad \text{Hom}(G_L, \mu_p) \rightarrow H^1(G_L, \text{Aut}(J)) \rightarrow \text{Twist}(J/L),$$

where the first map is given by the map $\mu_p \rightarrow \text{Aut}(J)$ in Remark 1.2. The last map is the bijection given above. A p -twist of J by $\chi \in \mathcal{C}^p(K)$ is then, given by the image of χ in (3).

2. COMPARISON OF LOCAL CONDITIONS

In this section, let $C_{p,f}$ denote a superelliptic curve defined over a local field K_v containing the p -th roots of unity, where $n := \deg(f)$, so that $\text{Gal}(f) \subset S_n$. For the rest of the paper, a local field is either an archimedean field, or a finite extension of \mathbf{Q}_ℓ for some prime number ℓ . If K_v is an archimedean field, we write $v|\infty$, and if the residue characteristic of K_v is p , we write $v|p$. Let 1_v denote the trivial character in $\mathcal{C}^p(K_v)$. We denote the Jacobian of $C_{p,f}$ simply by J . The local conditions in Definition 2.2 are in fact those of the π -Selmer group (to be defined later) of the Jacobian of a superelliptic curve defined over a number field. In this section, we list several lemmas to be used in the sequel.

Definition 2.1. Let V be a finite dimensional vector space over \mathbf{F}_p . We write $d_p(V)$ for the dimension of V over \mathbf{F}_p .

Definition 2.2. For $\chi \in \mathcal{C}^p(K_v)$, define

$$\alpha_v(\chi) := \text{Im}(J^\chi(K_v)/\pi J^\chi(K_v) \rightarrow H^1(K_v, J^\chi[\pi]) \cong H^1(K_v, J[\pi])),$$

where the first map is given by the Kummer map. Define

$$h_v(\chi) := d_p(\alpha_v(1_v)/(\alpha_v(1_v) \cap \alpha_v(\chi))).$$

The vector space $\alpha_v(\chi)$ and the invariant $h_v(\chi)$ certainly depend on $C_{p,f}$ and the field K_v over which $C_{p,f}$ is defined, but we suppress them from the notation.

Let $\lambda : J \rightarrow \hat{J}$ be the canonical principal polarization. Then $J[\pi]$ is self-dual; i.e., $\lambda^{-1}(\hat{J}[\hat{\pi}]) = J[\pi]$, where $\hat{\pi}$ is the dual isogeny of π (see [15, Proposition 3.1]). Let $\langle \cdot, \cdot \rangle_\pi$ denote the Cartier pairing (for example, see Section 1 in [12]) for $\pi : J \rightarrow J$ (multiplication by π).

Definition 2.3. Define a pairing

$$e_\pi : J[\pi] \times J[\pi] \rightarrow \mu_p$$

by sending (x, y) to $\langle x, \lambda(y) \rangle_\pi$.

Remark 2.4. By properties of the Cartier pairing, the pairing e_π is bilinear, nondegenerate, and G_K -equivariant. In fact, e_π can be defined more concretely as follows. If e_p is the Weil pairing of $J[p]$ associated to the canonical principal polarization λ ,

$$e_\pi(a, b) := e_p(a, (\pi^{p-2})^{-1}(b)),$$

which can be proved by using functoriality in [12, Corollary 1.3(ii)]. If $p = 2$, then e_π is nothing but the Weil pairing of $J[2]$ associated to the canonical principal polarization.

The following theorem follows from Tate's local duality.

Theorem 2.5. *Tate's local duality and the pairing e_π give a nondegenerate pairing*

$$(4) \quad \langle \cdot, \cdot \rangle_v : H^1(K_v, J[\pi]) \times H^1(K_v, J[\pi]) \longrightarrow H^2(K_v, \zeta_p) = \mathbf{F}_p.$$

If $p = 2$, then the pairing is symmetric.

Proof. For example, see [11, Theorem 7.2.6]. The last assertion holds because the pairings given by cup product and the Weil pairings are alternating. \square

Lemma 2.6. *Let $C_{p,f}$ be a superelliptic curve over a local field K_v containing ζ_p . Then the image of the Kummer map*

$$J(K_v)/\pi J(K_v) \rightarrow H^1(K_v, J[\pi])$$

is its own orthogonal complement under pairing (4).

Proof. We prove it by applying the well-known fact that the image of the Kummer map

$$J(K_v)/pJ(K_v) \rightarrow H^1(K_v, J[p])$$

is self-dual in Tate's local duality for $H^1(K_v, J[p])$ and diagram chasing. By applying long exact sequences to the following diagrams

$$\begin{array}{ccccccc} 0 & \longrightarrow & J[\pi] & \longrightarrow & J & \xrightarrow{\pi} & J \longrightarrow 0 \\ & & \downarrow & & \parallel & & \downarrow p/\pi \\ 0 & \longrightarrow & J[p] & \longrightarrow & J & \xrightarrow{p} & J \longrightarrow 0 \end{array} \quad \begin{array}{ccccccc} 0 & \longrightarrow & J[\pi] & \longrightarrow & J & \xrightarrow{\pi} & J \longrightarrow 0 \\ & & \uparrow \pi^{p-2} & & \uparrow \pi^{p-2} & & \uparrow u \\ 0 & \longrightarrow & J[p] & \longrightarrow & J & \xrightarrow{p} & J \longrightarrow 0 \end{array}$$

we get the following commutative diagrams with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & J(K_v)/\pi J(K_v) & \xrightarrow{\phi} & H^1(K_v, J[\pi]) & \xrightarrow{\lambda} & H^1(K_v, J)[\pi] \longrightarrow 0 \\ & & \downarrow p/\pi & & \downarrow s & & \downarrow s' \\ 0 & \longrightarrow & J(K_v)/pJ(K_v) & \xrightarrow{\phi'} & H^1(K_v, J[p]) & \xrightarrow{\lambda'} & H^1(K_v, J)[p] \longrightarrow 0 \end{array}$$

$$\begin{array}{ccc} J(K_v)/\pi J(K_v) & \xrightarrow{\phi} & H^1(K_v, J[\pi]) \\ \uparrow u & & \uparrow \pi^{p-2} \\ J(K_v)/pJ(K_v) & \xrightarrow{\phi'} & H^1(K_v, J[p]), \end{array}$$

where ϕ and ϕ' are the Kummer maps and s, s' are natural maps. Let $\text{Im}(\phi)$ denote the set of the image of the map ϕ . We want to show that $\text{Im}(\phi) = \text{Im}(\phi)^\perp$. First we show that $\text{Im}(\phi) \subset \text{Im}(\phi)^\perp$; i.e., $\text{Im}(\phi) \perp \text{Im}(\phi)$. We have $\text{Im}(s \circ \phi) \subset \text{Im}(\phi')$ and $\text{Im}(\pi^{p-2} \circ \phi') = \text{Im}(\phi \circ u) = \text{Im}(\phi)$ since the map u is surjective. By the fact that $\text{Im}(\phi') \perp \text{Im}(\phi')$, we obtain $s^{-1}(\text{Im}(\phi')) \perp \text{Im}(\pi^{p-2} \circ (\phi'))$ because the following diagram commutes

$$\begin{array}{ccc} H^1(K_v, J[\pi]) & \times & H^1(K_v, J[\pi]) \xrightarrow{\cup} H^2(K_v, \mu_p) \\ \downarrow s & & \uparrow \pi^{p-2} \quad \parallel \\ H^1(K_v, J[p]) & \times & H^1(K_v, J[p]) \xrightarrow{\cup} H^2(K_v, \mu_p). \end{array}$$

Therefore $\text{Im}(\phi) \perp \text{Im}(\phi)$, or equivalently $\text{Im}(\phi) \subset \text{Im}(\phi)^\perp$. Next we show $\text{Im}(\phi)^\perp \subset \text{Im}(\phi)$. Let $b \in H^1(K_v, J[\pi])$ be an orthogonal element to $\text{Im}(\phi)$. Then

$$\begin{aligned} s(b) \perp (\pi^{p-2})^{-1}(\text{Im} \phi) &\Rightarrow s(b) \perp \text{Im}(\phi') \\ &\Rightarrow s(b) \in \text{Im}(\phi') \\ &\Rightarrow s(b) \in \ker(\lambda') \\ &\Rightarrow 0 = \lambda' \circ s(b) = s' \circ \lambda(b) \\ &\Rightarrow \lambda(b) = 0 \\ &\Rightarrow b \in \ker(\lambda) = \text{Im}(\phi). \end{aligned}$$

Hence we are done. \square

Remark 2.7. By Lemma 2.6 applied to J^χ , for $\chi \in \mathcal{C}^p(K_v)$, one can see that $\alpha_v(\chi)$ is its own orthogonal complement in (4). Since the pairing (4) is non-degenerate, we have

$$d_p(H^1(K_v, J[\pi])) = 2d_p(\alpha_v(\chi)).$$

Lemma 2.8. *Suppose that $v \nmid p\infty$ and J/K_v has good reduction. Then*

$$\alpha_v(1_v) \cong J[\pi]/(\text{Frob}_v - 1)J[\pi],$$

where the isomorphism is given by evaluating cocycles at a Frobenius automorphism Frob_v .

Proof. Under the assumption, we have an exact sequence

$$0 \longrightarrow J[\pi] \longrightarrow J(K_v^{\text{ur}}) \xrightarrow{\pi} J(K_v^{\text{ur}}) \longrightarrow 0,$$

where K_v^{ur} is the maximal unramified extension of K_v . Taking the long exact sequence, we get an exact sequence

$$0 \longrightarrow J(K_v)/\pi J(K_v) \longrightarrow H^1(K_v^{\text{ur}}/K_v, J[\pi]) \longrightarrow H^1(K_v^{\text{ur}}/K_v, J(K_v^{\text{ur}}))[\pi] \longrightarrow 0.$$

It is well-known that $H^1(K_v^{\text{ur}}/K_v, J(K_v^{\text{ur}})) = 0$ (e.g., see [9, proposition 1]). Hence

$$\alpha_v(1_v) \cong J(K_v)/\pi J(K_v) \cong H^1(K_v^{\text{ur}}/K_v, J[\pi]) \cong J[\pi]/(\text{Frob}_v - 1)J[\pi],$$

as wanted (for the last isomorphism, see [14, Lemma B.2.8]). \square

We identify $\alpha_v(1_v)$ with $J(K_v)/\pi J(K_v)$ in the proof of the Lemma below.

Lemma 2.9. *Suppose that $\chi \in \mathcal{C}^p(K_v)$, and $F_v := \overline{K}_v^{\ker(\chi)}$. Then we have*

$$(5) \quad \alpha_v(1_v) \cap \alpha_v(\chi) \supseteq (\mathbf{N}(J(F_v)) + \pi J(K_v))/\pi J(K_v),$$

where $\mathbf{N}(J(F_v))$ is the image of the norm map $J(F_v) \rightarrow J(K_v)$ and the intersection is taken in $H^1(K_v, J[\pi])$. In particular, if $\mathbf{N}(J(F_v)) = J(K_v)$, then $h_v(\chi) = 0$.

Proof. Consider the commutative diagrams

$$\begin{array}{ccc} J(F_v)/\pi J(F_v) & \longrightarrow & H^1(F_v, J[\pi]) \\ \uparrow i & & \uparrow \text{res} \\ J(K_v)/\pi J(K_v) & \longrightarrow & H^1(K_v, J[\pi]) \end{array} \quad \begin{array}{ccc} H^1(F_v, J[\pi]) & \longleftarrow & J(F_v)/\pi J(F_v) \\ \downarrow \text{cor} & & \downarrow \mathbf{N} \\ H^1(K_v, J[\pi]) & \longleftarrow & J(K_v)/\pi J(K_v) \end{array}$$

$$\begin{array}{ccc} H^1(F_v, J[\pi]) & \times & H^1(F_v, J[\pi]) \xrightarrow{\cup} H^2(F_v, \mu_p) \cong \mathbf{Z}/p\mathbf{Z} \\ \downarrow \text{cor} & & \uparrow \text{res} \\ H^1(K_v, J[\pi]) & \times & H^1(K_v, J[\pi]) \xrightarrow{\cup} H^2(K_v, \mu_p) \cong \mathbf{Z}/p\mathbf{Z} \end{array} \quad \begin{array}{c} \downarrow \text{cor} = \text{id} \end{array}$$

where i is the natural map and \mathbf{N} is induced by the norm map.

For convenience, let

$$\begin{aligned} A &= \alpha_v(1_v), \\ B &= \alpha_v(\chi), \text{ and} \\ D &= J(F_v)/\pi J(F_v) \cong J^\chi(F_v)/\pi J^\chi(F_v). \end{aligned}$$

By Lemma 2.6, we have $D = D^\perp \subseteq \text{res}(A)^\perp = \text{cor}^{-1}(A)$, and similarly, $D = D^\perp \subseteq \text{res}(B)^\perp = \text{cor}^{-1}(B)$. Therefore, $\mathbf{N}(D) = \text{cor}(D) \subseteq A \cap B$. \square

Lemma 2.10. *Let A be an abelian variety defined over K_v such that $\mathbf{Z}[\zeta_p] \subset \text{End}_{G_{K_v}}(A)$. Suppose that $v \nmid p\infty$. Then*

$$A(K_v)/\pi A(K_v) \cong A(K_v)[p^\infty]/\pi(A(K_v)[p^\infty]).$$

Proof. Multiplication by π is surjective on the pro-(prime to p) part of $A(K_v)$, so only the pro- p part $A(K_v)[p^\infty]$ contributes to $A(K_v)/\pi A(K_v)$, whence the result follows. \square

Lemma 2.11. *Suppose that $\chi \in \mathcal{C}^p(K_v)$, and $F_v = \overline{K}_v^{\ker(\chi)}$, where $v \nmid p\infty$. Then the following hold.*

- (i) $d_p(\alpha_v(1_v)) = d_p(J(K_v)/\pi J(K_v)) = d_p(J(K_v)[\pi])$.
- (ii) *Suppose further that, the extension F_v/K_v is ramified and J has good reduction. Then $J(K_v)/\pi J(K_v) \cong J(F_v)/\pi J(F_v)$.*

Proof. We have an exact sequence

$$0 \longrightarrow J(K_v)[\pi] \longrightarrow J(K_v)[p^\infty] \xrightarrow{\pi} J(K_v)[p^\infty] \longrightarrow J(K_v)[p^\infty]/\pi J(K_v)[p^\infty] \longrightarrow 0.$$

Hence (i) follows from Lemma 2.10.

Now we prove (ii). Under the assumptions, $K_v(J[p^\infty])$ is an unramified extension over K_v . Therefore $K_v(J(F_v)[p^\infty]) = K_v$, so $J(K_v)[p^\infty] = J(F_v)[p^\infty]$. Assertion (ii) follows from passing through (Lemma 2.10)

$$\begin{aligned} J(K_v)/\pi J(K_v) &\cong J(K_v)[p^\infty]/\pi(J(K_v)[p^\infty]) \\ &\cong J(F_v)[p^\infty]/\pi(J(F_v)[p^\infty]) \\ &\cong J(F_v)/\pi J(F_v). \end{aligned}$$

□

Lemma 2.12. *Suppose that $\sigma \in \text{Gal}(f) \subset S_n$ consists of b orbits. Let $J[\pi]^{\sigma=1}$ denote the subgroup of $J[\pi]$ which consists of the elements fixed by σ . Then*

$$d_p(J[\pi]^{\sigma=1}) = b - 1,$$

Proof. Let σ be $(\alpha_{11}\alpha_{12}\cdots\alpha_{1i_1})(\alpha_{21}\cdots\alpha_{2i_2})\cdots(\alpha_{b1}\cdots\alpha_{bi_b})$, where α_{xy} are the roots of f . We rearrange α_{xy} so that $p \nmid i_b$, which is always possible because $p \nmid n$. Let a_{xy} denote the divisor classes $[(\alpha_{xy}, 0) - \infty]$. Then with the equality $\sum a_{xy} = 0$ (Remark 1.2), one can show that

$$a_{11} + a_{12} + \cdots + a_{1i_1}, a_{21} + \cdots + a_{2i_2}, \dots, a_{(b-1)1} + \cdots + a_{b-1i_{b-1}}$$

form a basis of $J[\pi]^{\sigma=1}$.

□

Remark 2.13. Suppose that $v \nmid p\infty$. Let K_v^{ur} be the maximal unramified extension of K_v . It is well-known that if J/K_v has good reduction, then $J[\pi] \subset J[p] \subset J(K_v^{\text{ur}})$. Let Frob_v denote the Frobenius automorphism of K_v^{ur} . Restricting Frob_v to $K(J[\pi])$, one can regard Frob_v as an element in S_n by Remark 1.3.

Lemma 2.14. *Suppose that $v \nmid p\infty$, and J has a good reduction. Let b be the number of orbits of $\text{Frob}_v \in S_n$. Then*

$$d_p(\alpha_v(1_v)) = b - 1.$$

Proof. Note that $J(K_v)[\pi] = J[\pi]^{\text{Frob}_v=1}$. Then the lemma follows from Lemma 2.12 and Lemma 2.11.

□

Lemma 2.15. *Let $\chi \in \mathcal{C}^p(K_v)$. Suppose that χ satisfies one of the following conditions:*

- χ is trivial, or
- J has good reduction, $v \nmid p\infty$, and χ is unramified.

Then $h_v(\chi) = 0$.

Proof. Let $F_v = \overline{K}_v^{\ker(\chi)}$. In either case, $\mathbf{N}(J(F_v)) = J(K_v)$ (In second case, it follows from [6, Corollary 4.4]). Thus, by Lemma 2.9, $h_v(\chi) = 0$.

□

Lemma 2.16. *Suppose that $\chi \in \mathcal{C}^p(K_v)$, and $F_v := \overline{K}_v^{\ker(\chi)}$, where $v \nmid p\infty$. Suppose that $J(K_v)/\pi J(K_v) \cong J(F_v)/\pi J(F_v)$ (which is satisfied if the extension F_v/K_v is ramified and J has good reduction by Lemma 2.11). Then*

$$\alpha_v(1_v) \cap \alpha_v(\chi) = \{0\};$$

i.e., $h_v(\chi) = \dim_{\mathbf{F}_p}(J(K_v)[\pi])$.

Proof. Consider the following commutative diagrams

$$\begin{array}{ccc}
J(F_v)/\pi J(F_v) & \longrightarrow & H^1(F_v, J[\pi]) \\
\uparrow \cong \quad i & & \uparrow \text{res} \\
J(K_v)/\pi J(K_v) & \xrightarrow{j} & H^1(K_v, J[\pi])
\end{array}
\quad
\begin{array}{ccc}
H^1(F_v, J[\pi]) & \longleftarrow & J(F_v)/\pi J(F_v) \\
\downarrow \text{cor} & & \downarrow \mathbf{N} \\
H^1(K_v, J[\pi]) & \xleftarrow{j} & J(K_v)/\pi J(K_v)
\end{array}$$

as in the proof of Lemma 2.9. The map i in the diagrams is an isomorphism by assumptions. Let $a \in J(F_v)$. Then $a = \pi b + c$ where $b \in J(F_v)$ and $c \in J(K_v)$. Therefore

$$\mathbf{N}(a) = \pi \mathbf{N}(b) + pc \in \pi J(K_v).$$

This means the map \mathbf{N} in the diagrams is actually the zero map. Let

$$\begin{aligned}
A &:= J(K_v)/\pi J(K_v), \\
B &:= J^\times(K_v)/\pi J^\times(K_v), \text{ and} \\
D &:= J(F_v)/\pi J(F_v) \cong J^\times(F_v)/\pi J^\times(F_v),
\end{aligned}$$

for simplicity. From now on, we identify A, B and D with their Kummer images. We need to show that $A \cap B = \{0\}$. In other words, we want to show that $A + B (= (A \cap B)^\perp) = H^1(K_v, J[\pi])$. One inclusion is trivial. For the other inclusion, let x be an element in $H^1(K_v, J[\pi])$. According to third diagram in the proof of Lemma 2.9, we have $\text{res}^{-1}(D) = (\text{cor}(D))^\perp = 0^\perp = H^1(K_v, J[\pi])$, so we can find $y \in A$ such that $\text{res}(x - y) = 0$. Since $x - y \in \ker(\text{res})$, it is enough to show that

$$(6) \quad \ker(\text{res}) \subseteq A + B.$$

By the Inflation-Restriction Sequence,

$$\ker(\text{res}) \cong H^1(F_v/K_v, J[\pi]^{G_{F_v}}).$$

But actually, $J[\pi]^{G_{F_v}} = J(F_v)[\pi] = J(K_v)[\pi]$ by Lemma 2.11(i). Hence we have

$$(7) \quad \ker(\text{res}) \cong \text{Hom}(\text{Gal}(F_v/K_v), J(K_v)[\pi]).$$

Let $\psi : J \cong J^\times$ be an isomorphism defined over F_v . We have the following commutative diagram

$$\begin{array}{ccccc}
& & 0 & & \\
& & \downarrow & & \\
& & \text{Hom}(\text{Gal}(F_v/K_v), J(K_v)[\pi]) & & \\
& & \downarrow & & \\
J(K_v)/\pi J(K_v) & \xleftarrow{j} & H^1(K_v, J[\pi]) & \xleftarrow{j^\times} & J^\times(K_v)/\pi J^\times(K_v) \\
\downarrow & & \downarrow & & \downarrow \\
J(F_v)/\pi J(F_v) & \xleftarrow{\quad} & H^1(F_v, J[\pi]) & \xleftarrow{\quad} & J^\times(F_v)/\pi J^\times(F_v) \\
& \searrow \psi \simeq \swarrow & & &
\end{array}$$

where the middle column is exact. Define a homomorphism

$$\begin{aligned}\phi : J(K_v)[\pi] &\rightarrow \text{Hom}(\text{Gal}(F_v/K_v), J(K_v)[\pi]) \\ P &\mapsto j(\overline{P}) - j^\chi(\overline{\psi(P)}),\end{aligned}$$

where \overline{P} is the image of P in $J(K_v)/\pi J(K_v)$ and $\overline{\psi(P)}$ is the image of $\psi(P)$ in $J^\chi(K_v)/\pi J^\chi(K_v)$. That the map ϕ being well-defined can be shown by diagram chasing in the diagram above. We claim that the map ϕ is an isomorphism, which will imply (6). It is enough to show the map ϕ is injective since $J(K_v)[\pi]$ and $\text{Hom}(F_v/K_v, J(K_v)[\pi])$ have the same dimension over \mathbf{F}_p . It can be easily checked that for $P \neq 0$,

$$(j(\overline{P}) - j^\chi(\overline{\psi(P)}))(\tau) \neq 0,$$

where τ is a nontrivial element in $\text{Gal}(F_v/K_v)$, so we are done. \square

Until the end of this section, assume that $p = 2$. We show that the equality holds in (5) when $p = 2$. For the elliptic curve case, the following proposition is proved in [5, Proposition 7] and [7, Proposition 5.2].

Proposition 2.17. *Let $\chi \in \mathcal{C}^2(K_v)$. Then*

$$(8) \quad \alpha_v(1_v) \cap \alpha_v(\chi) = \mathbf{N}J(L_v)/2J(K_v),$$

where $L_v = \overline{K_v}^{\ker(\chi)}$, and $\mathbf{N}J(L_v)$ is the image of the norm map $\mathbf{N} : J(L_v) \rightarrow J(K_v)$.

The following two lemmas are used to prove the proposition.

Lemma 2.18. *Suppose that $\chi \in \mathcal{C}^2(K_v)$ is a nontrivial quadratic character, and $L_v := \overline{K_v}^{\ker(\chi)}$. Let*

$$\phi : H^1(K_v, J[2]) \rightarrow H^1(L_v, J[2])$$

be the restriction map. Then (i) $\ker(\phi) \subseteq \alpha_v(1_v) + \alpha_v(\chi)$, and (ii) $d_2(\ker(\phi)) = 2d_2(J(K_v)[2]) - d_2(J(L_v)[2])$.

Proof. Let

$$\begin{aligned}i : J(K_v)/2J(K_v) &\rightarrow H^1(K_v, J[2]), \text{ and} \\ i^\chi : J^\chi(K_v)/2J^\chi(K_v) &\rightarrow H^1(K_v, J^\chi[2]) \cong H^1(K_v, J[2]).\end{aligned}$$

By the Inflation-Restriction Sequence,

$$\ker(\phi) = H^1(L_v/K_v, J(L_v)[2]) = J(K_v)[2]/(\tau - 1)J(L_v)[2],$$

where $\text{Gal}(L_v/K_v)$ is generated by τ . Then for any $P \in J(K_v)[2]$, its image c_P in $H^1(K_v, J[2])$ of the composition map

$$J(K_v)[2] \rightarrow J(K_v)[2]/(\tau - 1)J(L_v)[2] \subset H^1(K_v, J[2])$$

is given by $c_P(\sigma) = P$ if $\sigma|_{L_v} = \tau$, and $c_P(\sigma) = 0$ otherwise. With the isomorphism $J(\overline{K_v}) \cong J^\chi(\overline{K_v})$, it is straightforward to check that $i(\overline{P}) + i^\chi(\overline{P^\chi}) = c_P$, where \overline{P} and $\overline{P^\chi}$ represent the images of P in $J(K_v)/2J(K_v)$ and $J^\chi(K_v)/2J^\chi(K_v)$, respectively. This proves (i). The exact sequence

$$0 \longrightarrow J(K_v)[2] \longrightarrow J(L_v)[2] \xrightarrow{\tau-1} J(K_v)[2] \longrightarrow \ker(\phi) \longrightarrow 0$$

shows (ii). \square

Lemma 2.19. *Let L_v/K_v be a nontrivial quadratic extension. Then*

$$2d_2(J(K_v)[2]) - d_2(J(L_v)[2]) = 2d_2(J(K_v)/2J(K_v)) - d_2(J(L_v)/2J(L_v)).$$

Proof. Consider the following diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J^\chi(K_v) & \longrightarrow & J(L_v) & \xrightarrow{N} & J(K_v) & \longrightarrow & J(K_v)/N(J(L_v)) & \longrightarrow & 0 \\ & & \downarrow 2 & & \downarrow 2 & & \downarrow 2 & & \downarrow 2 & & \\ 0 & \longrightarrow & J^\chi(K_v) & \longrightarrow & J(L_v) & \xrightarrow{N} & J(K_v) & \longrightarrow & J(K_v)/N(J(L_v)) & \longrightarrow & 0. \end{array}$$

Note that each row consists of two short exact sequences

$$\begin{aligned} 0 &\longrightarrow J^\chi(K_v) \longrightarrow J(L_v) \xrightarrow{N} NJ(L_v) \longrightarrow 0, \text{ and} \\ 0 &\longrightarrow NJ(L_v) \longrightarrow J(K_v) \longrightarrow J(K_v)/N(J(L_v)) \longrightarrow 0. \end{aligned}$$

Then applying the snake lemma for each short exact sequence and comparing the dimensions over \mathbf{F}_2 together with Proposition 1.7 and Remark 2.7 show the result. \square

Proof of Proposition 2.17. If L_v/K_v is trivial, then it is obvious. Thus assume L_v/K_v is a nontrivial quadratic extension. By Lemma 2.9, it is enough to show that

$$(9) \quad d_2(\alpha_v(1_v) \cap \alpha_v(\chi)) = d_2(\mathbf{N}J(L_v)/2J(K_v)).$$

Consider the following exact sequence ($M := J(K_v) + J^\chi(K_v) + 2J(L_v)$)

$$0 \longrightarrow M/2J(L_v) \longrightarrow J(L_v)/2J(L_v) \xrightarrow{\mathbf{N}} J(K_v)/2J(K_v) \longrightarrow J(K_v)/N(J(L_v)) \longrightarrow 0,$$

where the middle map \mathbf{N} is induced by the norm map and $J^\chi(K_v)$ is regarded as a subgroup of $J(L_v)$. For simplicity, write X, Y, Z and W for the nontrivial terms in the exact sequence in order. Let $A = \alpha_v(1_v)$, and $B = \alpha_v(\chi)$. Then $d_2(A+B) + d_2(A \cap B) = d_2(H^1(K_v, J[2]))$ since $A \cap B$ is the orthogonal complement of $A + B$ in (4). Let

$$\phi : H^1(K_v, J[2]) \rightarrow H^1(L_v, J[2])$$

be the restriction map. We have $X = \phi(A + B)$, so by Remark 2.7, Lemma 2.18, and Lemma 2.19,

$$\begin{aligned} d_2(X) &= d_2(A + B) - d_2(\ker(\phi)) \\ &= d_2(H^1(K_v, J[2])) - d_2(A \cap B) - d_2(\ker(\phi)) \\ &= d_2(H^1(K_v, J[2])) - d_2(A \cap B) - 2d_2(J(K_v)[2]) + d_2(J(L_v)[2]) \\ &= d_2(J(L_v)/2J(L_v)) - d_2(A \cap B). \end{aligned}$$

Then the equality $d_2(X) + d_2(Z) = d_2(Y) + d_2(W)$ shows (9), as desired. \square

For the following lemma, we specify v_0 so that $K_{v_0} = \mathbf{R}$.

Lemma 2.20. *Let $C_{2,f}$ be a hyperelliptic curve over the real field \mathbf{R} . Let η be the sign character. Suppose that f has $2k_1 - 1$ real roots and $2k_2$ complex roots. Then*

- (i) $J(\mathbf{R}) \cong (\mathbf{R}/\mathbf{Z})^{k_1+k_2-1} \oplus (\mathbf{Z}/2\mathbf{Z})^{k_1-1}$, and
- (ii) $h_{v_0}(\eta) = k_1 - 1$

Proof. Complex conjugation corresponds to the element of S_n that consists of $2k_1 - 1$ cycles of length 1 and k_2 cycles of length 2. Hence [10, Remark I.3.7] and Lemma 2.12 show (i). Note that the image of the norm map $\mathbf{N} : J(\mathbf{C}) \rightarrow J(\mathbf{R})$ is the connected component of 0 ($= (\mathbf{R}/\mathbf{Z})^{k_1+k_2-1}$) according to [10, Remark I.3.7]. Then (ii) follows from Proposition 2.17. \square

3. SELMER GROUPS AND CONTROLLING THE LOCALIZATION MAP

Let $C_{p,f}$ be a superelliptic curve over a number field K containing ζ_p , where $n = \deg(f)$ is not divisible by p . Let v be a place of K . We write K_v for the completion of K at v . For the rest of the paper, for every prime \mathfrak{q} , we fix an embedding $\overline{K} \hookrightarrow \overline{K}_{\mathfrak{q}}$, so that $G_{K_{\mathfrak{q}}} \subset G_K$. As usual, we write J for the Jacobian of $C_{p,f}$. Recall that $\text{Gal}(f) \in S_n$ has a natural action on $J[\pi]$ (Remark 1.3).

Definition 3.1. Let $\chi \in \mathcal{C}^p(K)$. The π -Selmer group $\text{Sel}_{\pi}(J^{\chi}/K) \subset H^1(K, J[\pi])$ is the (finite) \mathbf{F}_p -vector space defined by the following exact sequence

$$0 \longrightarrow \text{Sel}_{\pi}(J^{\chi}/K) \longrightarrow H^1(K, J[\pi]) \longrightarrow \bigoplus_v H^1(K_v, J[\pi])/\alpha_v(\chi_v),$$

where the rightmost map is the direct sum of the restriction maps, and χ_v is the restriction of χ to G_{K_v} .

Lemma 3.2. Suppose that $p \nmid n$. Then $H^1(S_n, J[\pi]) = 0$.

Proof. We regard S_n as the symmetric group on the set $\{1, 2, \dots, n\}$. Let $H := \{\sigma \in S_n \mid \sigma(n) = n\} \cong S_{n-1} \subset S_n$. We have an S_n -module isomorphism

$$\text{Ind}_H^{S_n} \mathbf{F}_p \cong \mathbf{F}_p[S_n/H]$$

where $\text{Ind}_H^{S_n} \mathbf{F}_p$ denote the induced S_n -module of the H -module \mathbf{F}_p (trivial action of H on \mathbf{F}_p). Let β_i be $(i \ n)$ in $\mathbf{F}_p[S_n/H]$. Note that $\sigma(\beta_i) = \beta_{\sigma(i)}$ in S_n/H . We put

$$D = \{a(\beta_1 + \beta_2 + \dots + \beta_n) \mid a \in \mathbf{F}_p\}.$$

Then

$$\text{Ind}_H^{S_n} \mathbf{F}_p/D \cong \mathbf{F}_p[S_n/H]/D \cong J[\pi].$$

In the last isomorphism the map is defined by $\beta_i \mapsto \alpha_i$ where α_i are the roots of polynomial of the given superelliptic curve. We have an $(S_n$ -module) exact sequence

$$(10) \quad 0 \longrightarrow D \xrightarrow{j} \text{Ind}_H^{S_n} \mathbf{F}_p \longrightarrow \text{Ind}_H^{S_n} \mathbf{F}_p/D \longrightarrow 0$$

But since $p \nmid n$, we have a map

$$g : \text{Ind}_H^{S_n} \mathbf{F}_p \longrightarrow D$$

defined by $a_1\beta_1 + \dots + a_n\beta_n \mapsto n^{-1}(a_1 + \dots + a_n)(\beta_1 + \dots + \beta_n)$ where n^{-1} is taken in $(\mathbf{Z}/p\mathbf{Z})^{\times}$. Clearly $g \circ j = \text{id}_D$, so the exact sequence (10) splits. Hence

$$H^1(S_n, \text{Ind}_H^{S_n} \mathbf{F}_p) \cong H^1(S_n, D) \oplus H^1(S_n, J[\pi]).$$

By Shapiro's lemma, $H^1(S_n, \text{Ind}_H^{S_n} \mathbf{F}_p) \cong H^1(H, \mathbf{F}_p)$. If p is odd, $H^1(H, \mathbf{F}_p) = \text{Hom}(H, \mathbf{F}_p) = 0$. If $p = 2$ (so $n \geq 3$), $H^1(H, \mathbf{F}_2) = \mathbf{Z}/2\mathbf{Z} = \text{Hom}(S_n, D) = H^1(S_n, D)$. In either case, we have $H^1(S_n, J[\pi]) = 0$. \square

Definition 3.3. We say that $C_{p,f}$ satisfies $(*)$ if one of the following holds.

- $p = 2$, $\text{Gal}(f) \cong A_n$ or S_n , and $n \geq 5$.
- $p = 2$, $n = 3$, and $\text{Gal}(f) \cong S_3$.

- p is an odd prime, and $\text{Gal}(f) \cong S_n$.

If $c \in H^1(K, J[\pi])$ and $\sigma \in G_K$, let

$$c(\sigma) \in J[\pi]/(\sigma - 1)J[\pi]$$

denote the image of σ under any cocycle representing c .

Lemma 3.4. *Let N be a finite subgroup of $H^1(K, J[\pi])$ and $\sigma \in G_K$. Suppose that $\phi : N \rightarrow J[\pi]/(\sigma - 1)J[\pi]$ is a homomorphism. Suppose that $\text{Gal}(K(J[\pi])/K) = \text{Gal}(f) = \Omega$ satisfies the following conditions.*

- (i) $H^1(\Omega, J[\pi]) = 0$,
- (ii) $J[\pi]$ is a simple Ω -module,
- (iii) $\dim_{\mathbb{F}_p}(\text{Hom}_{\Omega}(J[\pi], J[\pi])) = 1$, and
- (iv) Ω does not act on $J[\pi]$ trivially.

Then there exists an element $\rho \in G_K$ such that $\rho|_{K(J[\pi])^{K^{ab}}} = \sigma|_{K(J[\pi])^{K^{ab}}}$ and $c(\rho) = \phi(c)$ for all $c \in N$. In particular, if $C_{p,f}$ satisfies (), then there exists such an element $\rho \in G_K$.*

Proof. The proof of Lemma 3.5 of [8] works here, too. For the last assertion, it is not difficult to check that (ii), (iii), and (iv) are satisfied when $C_{p,f}$ satisfies (*). If $\text{Gal}(f) \cong S_n$, the condition (i) is Lemma 3.2. If $p = 2$, and $\text{Gal}(f) \cong A_n$, then $J[2]^{A_n=1} = 0$. The Hochschild-Serre Spectral Sequence (for example, see [11, Proposition 1.6.7]) together with the fact that $H^1(S_n, J[2]) = 0$ shows that $H^1(A_n, J[2])^{S_n/A_n=1} = 0$. Then $H^1(A_n, J[2]) = 0$ by the following fact that can be proved by a standard argument of group theory: If U, V are nontrivial 2-groups such that U acts on V , then V^U (:=the group of elements in V fixed by every element in U) is non-trivial. \square

Remark 3.5. Note that if C_f is an elliptic curve, and $\text{Gal}(f) \cong A_3$, the condition (iii) in Lemma 3.4 does not hold.

Definition 3.6. For every place v of K , we write res_v for the restriction map (fixing an embedding $\overline{K} \hookrightarrow \overline{K}_v$)

$$\text{res}_v : H^1(K, J[\pi]) \rightarrow H^1(K_v, J[\pi]).$$

Suppose that J has good reduction at $\mathfrak{q} \nmid p\infty$. Define the localization map

$$\text{loc}_{\mathfrak{q}} : \text{Sel}_{\pi}(J/K) \rightarrow \alpha_{\mathfrak{q}}(1_{\mathfrak{q}}) \cong J[\pi]/(\text{Frob}_{\mathfrak{q}} - 1),$$

where the former map is $\text{res}_{\mathfrak{q}}$ and the latter map given in Lemma 2.8. Note that $\text{loc}_{\mathfrak{q}}$ is given by evaluating cocycles at a Frobenius automorphism $\text{Frob}_{\mathfrak{q}}$.

We define various Selmer groups as follows.

Definition 3.7. Let \mathfrak{q} be a prime of K and $\psi_{\mathfrak{q}} \in \mathcal{C}^p(K_{\mathfrak{q}})$. Define

$$\begin{aligned} \text{Sel}_{\pi}(J, \psi_{\mathfrak{q}}) := \{x \in H^1(K, J[\pi]) \mid \text{res}_v(x) \in \alpha_v(1_v) \text{ if } v \neq \mathfrak{q}, \text{ and} \\ \text{res}_{\mathfrak{q}}(x) \in \alpha_{\mathfrak{q}}(\psi_{\mathfrak{q}})\}. \end{aligned}$$

Define

$$\begin{aligned} \text{Sel}_{\pi, \mathfrak{q}}(J/K) := \{x \in H^1(K, J[\pi]) \mid \text{res}_v(x) \in \alpha_v(1_v) \text{ if } v \neq \mathfrak{q}, \text{ and} \\ \text{res}_{\mathfrak{q}}(x) = 0\}. \end{aligned}$$

Define

$$\mathrm{Sel}_\pi^q(J/K) := \ker(H^1(K, J[\pi]) \rightarrow \bigoplus_{v \neq q} H^1(K_v, J[\pi])/\alpha_v(1_v)).$$

Obviously, $\mathrm{Sel}_{\pi,q}(J/K) \subseteq \mathrm{Sel}_\pi(J/K) \subseteq \mathrm{Sel}_\pi^q(J/K)$.

Lemma 3.8. *The right hand restriction maps of the following exact sequences are orthogonal complements under (4).*

$$0 \longrightarrow \mathrm{Sel}_\pi(J/K) \longrightarrow \mathrm{Sel}_\pi^q(J/K) \longrightarrow H^1(K_v, J[\pi])/\alpha_q(1_q),$$

$$0 \longrightarrow \mathrm{Sel}_{\pi,q}(J/K) \longrightarrow \mathrm{Sel}_\pi(J/K) \longrightarrow \alpha_q(1_q).$$

In particular, $d_p(\mathrm{Sel}_\pi^q(J/K)) - d_p(\mathrm{Sel}_{\pi,q}(J/K)) = d_p(\alpha_q(1_q)) = \frac{1}{2}d_p(H^1(K_q, J[\pi]))$.

Proof. The lemma follows from the Global Poitou-Tate Duality. For example, see [14, Theorem 1.7.3]. \square

4. π -SELMER RANKS OF JACOBIANS OF SUPERELLIPTIC CURVES

We continue to assume that $C_{p,f}$ is a superelliptic curve over a number field K containing ζ_p . In this section, we assume that p is a prime and $\mathrm{Gal}(f) \cong S_n$, where $n = \deg(f)$ is not divisible by p . Let Σ denote a (finite) set of places which contains all places where J has bad reduction, all archimedean places, and all primes above p . We enlarge Σ , if necessary, so that $\mathrm{Pic}(\mathcal{O}_{K,\Sigma}) = 0$. As before, we write J for the Jacobian of $C_{p,f}$. In this section, we prove that if p is an odd prime, there exist infinitely many p -twists of J whose Jacobians have π -Selmer ranks equal to any non-negative integer r .

Remark 4.1. Note that our p -twists (Definition 1.5) of J over K are also Jacobians of superelliptic curves over K and that a p -twist of a p -twist is still a p -twist. This enables us to use an inductive argument. For example, if we have an algorithm to construct a p -twist of the Jacobian of a superelliptic curve having a strictly bigger π -Selmer group than the original π -Selmer group, we can make the π -Selmer group as big (the dimension over \mathbf{F}_p) as we want by taking p -twists.

Proposition 4.2. *Suppose that K is a number field containing ζ_p , and $f \in K[x]$ is a separable polynomial. Let $n = \deg(f)$ and suppose that $p \nmid n$ is an odd prime and $\mathrm{Gal}(f) \cong S_n$. Let $J := J(C_{p,f})$. Suppose that $d_p(\mathrm{Sel}_\pi(J/K)) \geq 1$. Then there exist infinitely many p -twists J^χ such that $d_p(\mathrm{Sel}_\pi(J^\chi/K)) = d_p(\mathrm{Sel}_\pi(J/K)) - 1$.*

Proof. We prove this proposition by following the method of the proof of [8, Proposition 5.1]. Let Δ_f be the discriminant of the polynomial f . Let θ be the (formal) product of p^3 , all primes where J has bad reduction and all archimedean places. Let $K(\theta)$ be its ray class field and $K[\theta]$ be the p -maximal subextension of $K(\theta)$. Then, $K[\theta]$ and $K(J[\pi])$ are linearly disjoint. Indeed, S_n has no normal subgroup of index p for an odd prime p . Therefore we can find an element $\sigma \in G_K$ such that $\sigma|_{K(J[\pi])}$ consists of 2 disjoint orbits $(\sigma|_{K(J[\pi])} \in \mathrm{Gal}(K(J[\pi])/K) = \mathrm{Gal}(f) = S_n)$, and $\sigma|_{K[\theta]} = 1$.

Let

$$\phi : \mathrm{Sel}_\pi(J/K) \longrightarrow J[\pi]/(\sigma - 1)J[\pi]$$

be a homomorphism. By Lemma 3.4, we can find $\rho \in G_K$ such that

$$\bullet \quad \rho|_{K[\theta]K(J[\pi])} = \sigma$$

- $c(\rho) = \phi(c)$ for every $c \in \text{Sel}_\pi(J/K)$.

Let N be a Galois extension of K containing $K(\theta)K(J[\pi])$, large enough so that the restriction of every element in $\text{Sel}_\pi(J/K)$ to G_N is zero (Choosing such a G_N is possible because the Selmer group is finite).

By the Chebotarev density theorem, we can find a prime \mathfrak{q} of K such that $\mathfrak{q} \nmid p$, J has good reduction at \mathfrak{q} , the extension N/K is unramified at \mathfrak{q} and $\text{Frob}_\mathfrak{q} \in$ (the conjugacy class of ρ in $\text{Gal}(N/K)$). Since $p \nmid [K(\theta) : K[\theta]]$, the restriction of ρ^k to $K(\theta)$ is trivial for some $p \nmid k$. Therefore \mathfrak{q}^k is principal generated by $d \equiv 1 \pmod{\theta}$. Let $F = K(\sqrt[p]{d})$. Then all places dividing θ split in F/K , the extension F/K is ramified at \mathfrak{q} , and nowhere else because its discriminant divides $p^p d^{p-1}$. Let χ denote the image of the Kummer map $K^\times / (K^\times)^p \cong \mathcal{C}^p(K)$. Therefore, by Lemma 2.15, $\alpha(1_v) = \alpha(\chi_v)$ for all places v except \mathfrak{q} , where χ_v is the restriction of χ to G_{K_v} .

Since J has good reduction at \mathfrak{q} ,

$$\alpha_\mathfrak{q}(1_\mathfrak{q}) \cong J[\pi]/(\text{Frob}_\mathfrak{q} - 1)J[\pi] \cong J[\pi]/(\rho - 1)J[\pi] = J[\pi]/(\sigma - 1)J[\pi].$$

The first isomorphism follows from Lemma 2.8. By Lemma 2.14 and our choice of σ , we have $d_p(\alpha_\mathfrak{q}(1_\mathfrak{q})) = 1$.

The localization map (Definition 3.6)

$$\text{loc}_\mathfrak{q} : \text{Sel}_\pi(J/K) \longrightarrow \alpha_\mathfrak{q}(1_\mathfrak{q}) \cong J[\pi]/(\rho - 1)J[\pi]$$

is given by evaluation of cocycles at $\text{Frob}_\mathfrak{q} \sim \rho$. Therefore we have

$$\text{loc}_\mathfrak{q}(\text{Sel}_\pi(J/K)) = \phi(\text{Sel}_\pi(J/K))$$

by Lemma 3.4. Note that $d_p(\text{Sel}_\pi^\mathfrak{q}(J/K)) - d_p(\text{Sel}_{\pi,\mathfrak{q}}(J/K)) = 1$ by Lemma 3.8. Choose ϕ so that $d_p(\text{Im}(\phi)) = 1$. Then, $\text{Sel}_\pi(J/K) = \text{Sel}_\pi^\mathfrak{q}(J/K)$. Then Lemma 2.16 and Lemma 3.8 show that

$$d_p(\text{Sel}_\pi(J^\chi/K)) = d_p(\text{Sel}_\pi(J/K)) - 1.$$

□

Definition 4.3. Let θ be a (formal) product of primes of K . Define

$$\Sigma(\theta) := \Sigma \cup \{\mathfrak{q} : \mathfrak{q}|\theta\},$$

$$\mathcal{P}_i := \{\mathfrak{q} : \mathfrak{q} \notin \Sigma \text{ and } \dim_{\mathbf{F}_p}(J[\pi]^{G_{K_\mathfrak{q}}}) = i\} \quad \text{for } 0 \leq i \leq n-1, \text{ and}$$

$$\mathcal{P} := \mathcal{P}_0 \coprod \mathcal{P}_1 \coprod \mathcal{P}_2 \coprod \cdots \coprod \mathcal{P}_{n-1} = \{\mathfrak{q} : \mathfrak{q} \notin \Sigma\}.$$

Remark 4.4. If $\mathfrak{q} \in \mathcal{P}_i$, then $d_p(\alpha_\mathfrak{q}(1_\mathfrak{q})) = i$ by Lemma 2.11.

Lemma 4.5. Suppose that v is a prime of K such that $v \nmid p\infty$, and J has good reduction at v . If $\psi_v \in \mathcal{C}_{\text{ram}}^p(K_v)$, then

$$J^{\psi_v}(K_v)[p^\infty] = J^{\psi_v}(K_v)[\pi] \cong J(K_v)[\pi]$$

Proof. Let $L_v := \overline{K}_v^{\text{Ker}(\psi_v)}$ so that L_v is a (totally) ramified extension over K_v of degree p . Let $K_v^{\text{ur}}, L_v^{\text{ur}}$ denote the maximal unramified extensions over K_v, L_v , respectively. It is sufficient to prove that

$$(11) \quad J^{\psi_v}(K_v^{\text{ur}})[p^\infty] = J^{\psi_v}(K_v^{\text{ur}})[\pi].$$

Let $\sigma \in \text{Gal}(L_v^{\text{ur}}/K_v^{\text{ur}})$ be non-trivial. Then

$$J^{\psi_v}(L_v^{\text{ur}})[p^\infty]^{\sigma=1} = J^{\psi_v}(K_v^{\text{ur}})[p^\infty].$$

It is well-known that the assumptions that $v \nmid p\infty$ and J has good reduction at v imply that $J[p^\infty] \subset J(K_v^{\text{ur}})$. Let

$$\lambda : J^{\psi_v} \cong J$$

be an isomorphism over L_v . Note that $\lambda^\sigma = \sigma\lambda\sigma^{-1} = \psi_v(\sigma)\lambda$. If $P \in J^{\psi_v}(K_v^{\text{ur}})[p^\infty]$, then

$$(12) \quad \lambda(P) = \lambda(P^\sigma) = \psi_v(\sigma)^{-1}\lambda^\sigma(P^\sigma) = \psi_v(\sigma)^{-1}(\lambda(P))^\sigma = \psi_v(\sigma)^{-1}\lambda(P),$$

whence $P = \zeta_p P$ if we take σ so that $\psi_v(\sigma) = \zeta_p^{-1}$. In the last equality in (12), we have used the fact that $J[p^\infty] \subset J(K_v^{\text{ur}})$. Now it is easy to see that (11) holds. \square

Definition 4.6. Choose a nontrivial unramified character $\epsilon_{\mathfrak{q}} \in \mathcal{C}^p(K_{\mathfrak{q}})$ and a ramified character $\eta_{\mathfrak{q}} \in \mathcal{C}_{\text{ram}}(K_{\mathfrak{q}})$ for every prime $\mathfrak{q} \in \mathcal{P}$. Define

$$\eta_{\mathfrak{q},j} := \eta_{\mathfrak{q}} \epsilon_{\mathfrak{q}}^j$$

for every $0 \leq j \leq p-1$.

Obviously, all $\eta_{\mathfrak{q},j}$ are in $\mathcal{C}_{\text{ram}}^p(K_{\mathfrak{q}})$.

Lemma 4.7. *Suppose that p is an odd prime. Let $\mathfrak{q} \in \mathcal{P}$ be a prime such that every orbit of $\text{Frob}_{\mathfrak{q}} \in S_n$ has length not divisible by p . Then for any a, b such that $0 \leq a, b \leq p-1$ and $a \neq b$,*

$$\alpha_{\mathfrak{q}}(\eta_{\mathfrak{q},a}) \cap \alpha_{\mathfrak{q}}(\eta_{\mathfrak{q},b}) = \{0\}.$$

Proof. Lemma 2.10 and Lemma 4.5 show that

$$\begin{aligned} J^{\eta_{\mathfrak{q},a}}(K_{\mathfrak{q}})/\pi J^{\eta_{\mathfrak{q},a}}(K_{\mathfrak{q}}) &\cong J^{\eta_{\mathfrak{q},a}}(K_{\mathfrak{q}})[p^\infty]/\pi J^{\eta_{\mathfrak{q},a}}(K_{\mathfrak{q}})[p^\infty] \\ &\cong J^{\eta_{\mathfrak{q},a}}(K_{\mathfrak{q}})[\pi]/\pi J^{\eta_{\mathfrak{q},a}}(K_{\mathfrak{q}})[\pi] \\ &= J^{\eta_{\mathfrak{q},a}}(K_{\mathfrak{q}})[\pi]. \end{aligned}$$

Let $F_{\mathfrak{q}} := \overline{K}_{\mathfrak{q}}^{\text{Ker } \epsilon_{\mathfrak{q}}^{b-a}}$, the degree p unramified extension over $K_{\mathfrak{q}}$. Since every orbit of $\text{Frob}_{\mathfrak{q}}$ has length not divisible by p , the degree $[K_{\mathfrak{q}}(J[\pi]) : K_{\mathfrak{q}}]$ is not as well. In particular, $F_{\mathfrak{q}}$ and $K_{\mathfrak{q}}(J[\pi])$ are linearly disjoint over $K_{\mathfrak{q}}$. Then it follows that

$$J^{\eta_{\mathfrak{q},a}}(F_{\mathfrak{q}})[\pi] \cong J(F_{\mathfrak{q}})[\pi] = J(K_{\mathfrak{q}})[\pi] \cong J^{\eta_{\mathfrak{q},a}}(K_{\mathfrak{q}})[\pi].$$

Hence we have

$$J^{\eta_{\mathfrak{q},a}}(F_{\mathfrak{q}})/\pi J^{\eta_{\mathfrak{q},a}}(F_{\mathfrak{q}}) \cong J^{\eta_{\mathfrak{q},a}}(F_{\mathfrak{q}})[\pi] = J^{\eta_{\mathfrak{q},a}}(K_{\mathfrak{q}})[\pi] \cong J^{\eta_{\mathfrak{q},a}}(K_{\mathfrak{q}})/\pi J^{\eta_{\mathfrak{q},a}}(K_{\mathfrak{q}}),$$

where the first isomorphism comes exactly as above. Finally, we apply Lemma 2.16 to get the conclusion. \square

Lemma 4.8. [4, Lemma 6.6] *Suppose that G, H are abelian groups and $M \subset G \times H$ is a subgroup. Let π_G and π_H denote the projection maps from $G \times H$ to G and H , respectively. Let $M_0 := \ker(\pi_G : M \rightarrow G/G^p)$.*

- (i) *The image of the natural map $\text{Hom}((G \times H)/M, \mu_p) \rightarrow \text{Hom}(H, \mu_p)$ is exactly $\{g \in \text{Hom}(H, \mu_p) : \pi_H(M_0) \subset \ker(g)\}$*
- (ii) *If $M/M^p \rightarrow G/G^p$ is injective, then $\text{Hom}((G \times H)/M, \mu_p) \rightarrow \text{Hom}(H, \mu_p)$ is surjective.*

Lemma 4.9. *Suppose that $\mathcal{O}_{\mathfrak{q}}$ is the ring of integers of $K_{\mathfrak{q}}$ for every prime ideal \mathfrak{q} . Then the natural map*

$$(13) \quad \mathcal{O}_{K,\Sigma}^{\times}/(\mathcal{O}_{K,\Sigma}^{\times})^p \longrightarrow \prod_{\mathfrak{q} \in \mathcal{P}_0} \mathcal{O}_{\mathfrak{q}}^{\times}/(\mathcal{O}_{\mathfrak{q}}^{\times})^p$$

is injective.

Proof. Let α be a nontrivial element of $\mathcal{O}_{K,\Sigma}^{\times}/(\mathcal{O}_{K,\Sigma}^{\times})^p$. We want to find a prime $\mathfrak{q}' \in \mathcal{P}_0$ such that $\alpha \notin (\mathcal{O}_{\mathfrak{q}'}^{\times})^p$. Two fields $K(\sqrt[p]{\alpha})$ and $K(J[\pi])$ are linearly disjoint over K because S_n doesn't have a normal subgroup of index p for an odd prime p . We choose an element $\tau \in G_K$ such that

- $\tau|_{K(\sqrt[p]{\alpha})} \neq 1$, and
- $\tau|_{K(J[\pi])} \in S_n$ is a n -cycle.

Let U be the conjugacy class of τ in $\text{Gal}(K(\sqrt[p]{\alpha})K(J[\pi])/K)$. By the Chebotarev density theorem, there exist infinitely many \mathfrak{q}' such that $\text{Frob}_{\mathfrak{q}'} \in U$. Such a prime \mathfrak{q}' satisfies both $\alpha \notin (\mathcal{O}_{\mathfrak{q}'}^{\times})^p$ and $\mathfrak{q}' \in \mathcal{P}_0$ if $\mathfrak{q}' \notin \Sigma$. \square

Remark 4.10. One can check easily that Lemma 4.9 still holds if we replace Σ by a finite set containing Σ .

Proposition 4.11. *Suppose that p is an odd prime. Then there are infinitely many prime ideals $\ell \in \mathcal{P}_1$ and an integer $0 \leq e \leq p-1$ so that*

$$(14) \quad d_p(\text{Sel}_{\pi}(J, \eta_{\ell,e})) = d_p(\text{Sel}_{\pi}(J/K)) + 1,$$

where $\eta_{\ell,e}$ is as in Definition 4.6.

Proof. Since $\text{Gal}(K(J[\pi])/K) \cong S_n$, we can find a prime $\ell \in \mathcal{P}_1$ (equivalently, Frob_{ℓ} has 2 orbits) such that neither of the order of the orbits of $\text{Frob}_{\ell} \in S_n$ is divisible by p (which is possible since p is an odd prime) and that the localization map (Definition 3.6)

$$\text{loc}_{\ell} : \text{Sel}_{\pi}(J/K) \longrightarrow \alpha_{\ell}(1_{\ell}) \cong J[\pi]/(\text{Frob}_{\ell} - 1)J[\pi]$$

is trivial by Lemma 3.4 combined with the Chebotarev Density Theorem. In other words, $\text{Sel}_{\pi}(J/K) = \text{Sel}_{\pi,\ell}(J/K)$. By Lemma 3.8, $\dim_{\mathbf{F}_p}(\text{Sel}_{\pi}^{\ell}(J/K)) = \dim_{\mathbf{F}_p}(\text{Sel}_{\pi,\ell}(J/K)) + 1$. Denote the image of the restriction map

$$\text{res}_{\ell} : \text{Sel}_{\pi}^{\ell}(J/K) \rightarrow H^1(K_{\ell}, J[\pi])$$

by $\text{res}_{\ell}(\text{Sel}_{\pi}^{\ell}(J/K))$. Then the set $\text{res}_{\ell}(\text{Sel}_{\pi}^{\ell}(J/K))$ is a 1-dimensional \mathbf{F}_p -vector subspace of $H^1(K_{\ell}, J[\pi])$. But Lemma 4.7, Lemma 2.16, and Lemma 2.15 together show that one can find a $\eta_{\ell,e} \in \mathcal{C}_{\text{ram}}^p(K_{\ell})$ such that

$$\text{res}_{\ell}(\text{Sel}_{\pi}^{\ell}(J/K)) = \alpha_{\ell}(\eta_{\ell,e}),$$

since there are exactly $p+1$ pairwise distinct 1-dimensional subspaces of $H^1(K_{\ell}, J[\pi])$ because $\ell \in \mathcal{P}_1$ (so $d_2(H^1(K_{\ell}, J[\pi])) = 2$). It follows that $\text{Sel}_{\pi}^{\ell}(J/K) = \text{Sel}_{\pi}(J, \eta_{\ell,e})$, so we are done. \square

Proposition 4.12. *Suppose that K is a number field containing ζ_p , and $f \in K[x]$ is a separable polynomial. Let $n = \deg(f)$ and suppose that $p \nmid n$ is an odd prime and $\text{Gal}(f) \cong S_n$. Let $J := J(C_{p,f})$. Then there exists infinitely many p -twists J^{\times} such that $d_p(\text{Sel}_{\pi}(J^{\times}/K)) = d_p(\text{Sel}_{\pi}(J/K)) + 1$.*

Proof. The main technique in the proof is already used in that of [4, Proposition 6.8]. Suppose that $\ell \in \mathcal{P}_1$ is as in Proposition 4.11. As stated earlier in this section we can enlarge Σ , if necessary, so that $\text{Pic}(\mathcal{O}_{K, \Sigma(\ell)}) = 0$. Thus global class field theory gives

$$\mathcal{C}^p(K) = \text{Hom}(\mathbf{A}_K^\times / K^\times, \mu_p) = \text{Hom}((\prod_{v \in \Sigma(\ell)} K_v^\times \times \prod_{q \notin \Sigma(\ell)} \mathcal{O}_q^\times) / \mathcal{O}_{K, \Sigma(\ell)}^\times, \mu_p).$$

Let $\psi_{\ell, e} \in \mathcal{C}_{\text{ram}}^p(K_\ell)$ be the character such that (14) holds. Define

$$\begin{aligned} Q &:= \mathcal{P} - \{\mathcal{P}_0 \cup \Sigma(\ell)\}, \\ M &:= \mathcal{O}_{K, \Sigma(\ell)}^\times, \\ G &:= \prod_{q \in \mathcal{P}_0} \mathcal{O}_q^\times, \text{ and} \\ H &:= \prod_{q \in Q} \mathcal{O}_q^\times \times \prod_{v \in \Sigma(\ell)} K_v^\times. \end{aligned}$$

By Remark 4.10, the map $M/M^p \rightarrow G/G^p$ is injective. Therefore

$$\begin{aligned} \mathcal{C}^p(K) = \text{Hom}((G \times H)/M, \mu_p) &\longrightarrow \text{Hom}(H, \mu_p) \\ &\cong \prod_{q \in Q} \text{Hom}(\mathcal{O}_q^\times, \mu_p) \times \prod_{v \in \Sigma(\ell)} \text{Hom}(K_v^\times, \mu_p) \end{aligned}$$

is surjective by Lemma 4.8. Since the map is surjective, there exists a $\chi \in \mathcal{C}^p(K)$ satisfying

- $\chi_\ell = \psi_{\ell, e}$,
- $\chi_q|_{\mathcal{O}_q^\times} = 1_q$ for $q \in Q$, and
- $\chi_v = 1_v$ for $v \in \Sigma$,

where $\chi_\ell, \chi_q, \chi_v$ are the restrictions of χ to $G_{K_\ell}, G_{K_q}, G_{K_v}$, respectively. Then in particular, χ_q is an unramified character if $q \in Q$. Note that by Lemma 2.15 the local conditions of two Selmer groups $\text{Sel}_\pi(J^\times/K)$ and $\text{Sel}_\pi(J/K)$ are the same except at ℓ , namely, $\alpha_{\mathfrak{p}}(\chi_{\mathfrak{p}}) = \alpha_{\mathfrak{p}}(1_p)$ for $\mathfrak{p} \neq \ell$. Therefore, $\text{Sel}_\pi(J^\times/K) = \text{Sel}_\pi(J, \eta_{\ell, e})$, so by Proposition 4.11,

$$d_p(\text{Sel}_\pi(J^\times/K)) = d_p(\text{Sel}_\pi(J/K)) + 1$$

□

Finally Proposition 4.2, Proposition 4.12, and induction show the following.

Theorem 4.13. *Suppose that K is a number field containing ζ_p , and $f \in K[x]$ is a separable polynomial. Let $n = \deg(f)$ and suppose that $p \nmid n$ is an odd prime and $\text{Gal}(f) \cong S_n$. Let $J := J(C_{p, f})$. Then for any nonnegative integer r , there exist infinitely many p -twists J^\times such that $d_p(\text{Sel}_\pi(J^\times/K)) = r$.*

5. CANONICAL QUADRATIC FORMS

Until the end of the paper, we are only interested in the hyperelliptic curve case, so we simply write C_f , and $\mathcal{C}(K)$ (or, $\mathcal{C}(K_v)$) to denote the hyperelliptic curve $C_{2, f}$ given by $y^2 = f(x)$, and $\mathcal{C}^2(K)$ (or, $\mathcal{C}^2(K_v)$), respectively. We denote the Jacobian of C_f by J . We give a proof of the fact that the two quadratic forms (defined below) on $J[2]$ and $J^\times[2]$ induced from the Heisenberg groups coincide. This enables us to show a parity relation between two Selmer groups $\text{Sel}_2(J/K)$ and $\text{Sel}_2(J^\times/K)$ (See Theorem 5.11).

Let V be a \mathbf{F}_2 -vector space. Following [4], we define quadratic forms, metabolic spaces, and Lagrangian (maximal isotropic) subspaces.

Definition 5.1. A *quadratic form* on V is a function $q : V \rightarrow \mathbf{F}_2$ such that

- $q(av) = a^2q(v)$ for every $a \in \mathbf{F}_2$ and $v \in V$, and
- the map $(v, w)_q := q(v + w) - q(v) - q(w)$ is a bilinear form.

We say that X is a *Lagrangian subspace* or *maximal isotropic subspace* of V if $q(X) = 0$ and $X = X^\perp$ in the induced bilinear form.

A *metabolic space* (V, q) is a vector space such that $(\cdot, \cdot)_q$ is nondegenerate and V contains a *Lagrangian subspace*.

Lemma 5.2. Suppose that (V, q) is a metabolic space such that $d_2(V) = 2n$. Then for a given Lagrangian subspace X of V , there are exactly $2^{n(n-1)/2}$ Lagrangian subspaces that intersect X trivially; i.e.,

$$|\{Y : Y \text{ is a Lagrangian subspace such that } Y \cap X = \{0\}\}| = 2^{n(n-1)/2}.$$

Proof. This is immediate from Proposition 2.6 (b),(c), and (e) in [13]. \square

The most interesting case for our purposes is when $V = H^1(K_v, J[2])$ for local fields K_v . In this case, there is a canonical way to construct a quadratic form $q_{\mathcal{H}}$ using the Heisenberg group defined below (for more general case, see [13, §4]). The associated bilinear form (Definition 5.1) given by such a quadratic form is the same as the pairing (4) (see [13, Corollary 4.7]). Then $\alpha_v(1_v)$ is a Lagrangian space by [13, Proposition 4.9], so $(H^1(K_v, J[2]), q_{\mathcal{H}})$ is a metabolic space. We explain the construction of $q_{\mathcal{H}}$ in more detail below. Following [2, Theorem A.8.1.1] we define a Theta (Weil) divisor.

Definition 5.3. Let C be a smooth projective curve of genus $g \geq 1$. If $j : C \rightarrow J(C)$ is an injection, define a Theta (Weil) divisor (depending on j) $\Theta_{J(C),j}$ by

$$\Theta_{J(C),j} := j(C) + \cdots + j(C) \text{ (} g-1 \text{ copies)}.$$

Remark 5.4. Our main interest is when C is a hyperelliptic curve C_f . In such case, we fix an embedding $j : C_f \rightarrow J$ by sending (x, y) to $[(x, y) - \infty]$. Then the Theta divisor Θ_J satisfies

$$[-1]^*\Theta_J = \Theta_J,$$

since $-[(x, y) - \infty] = [(x, -y) - \infty]$ in $\text{Pic}^0(C_f)(\cong J)$.

Now we define the Heisenberg group for $[2] : J \rightarrow J$.

Definition 5.5. The Heisenberg group $\mathcal{H}_{J,\Theta}$ is defined by

$$\mathcal{H}_{J,\Theta_J} := \{(x, g) : x \in J[2], \text{ and } g \in \mathbb{k}(J) \text{ such that } \text{div}(g) = 2\tau_x^*(\Theta_J) - 2\Theta_J\}$$

where τ_x is translation by x , and $\mathbb{k}(J)$ is the function field of J . The group operation is given by $(x, g)(x', g') = (x + x', \tau_{x'}^*(g)g')$.

Remark 5.6. By [13, Remark 4.5] and [2, Corollary A.8.2.3], we see that Definition 5.5 is a special case of the definition given in the paragraph just before [13, Proposition 4.6]. Let L be a field of characteristic 0, over which J is defined. There is an exact sequence

$$(15) \quad 1 \rightarrow \bar{L}^\times \rightarrow \mathcal{H}_{J,\Theta_J} \rightarrow J[2] \rightarrow 0,$$

where the middle maps are given by sending t to $(0, t)$, and by projection. Then a quadratic form $q_{\mathcal{H}}$ is given by the connecting homomorphism

$$H^1(L, J[2]) \rightarrow H^2(L, \bar{L}^\times).$$

Note that the construction of $q_{\mathcal{H}}$ is functorial with respect to base extension.

Definition 5.7. Let C_f be a hyperelliptic curve over a local field K_v . Let J be the Jacobian of C_f . Define

$$q_{J,v} : H^1(K_v, J[2]) \rightarrow H^2(K_v, \bar{K}_v^\times) \cong \mathbf{Q}/\mathbf{Z}$$

given by the connecting homomorphism of the exact sequence

$$1 \rightarrow \bar{K}_v^\times \rightarrow \mathcal{H}_{J,\Theta_J} \rightarrow J[2] \rightarrow 0.$$

Lemma 5.8. Let C_f be a hyperelliptic curve over a number field K . Suppose that $x \in H^1(K, J[2])$. Then

$$\sum_v q_{\mathcal{H},v}(\text{res}_v(x)) = 0,$$

where res_v is the restriction map from $H^1(K, J[2])$ to $H^1(K_v, J[2])$.

Proof. We have an exact sequence (see [11, Theorem 8.1.17] for reference)

$$0 \longrightarrow \text{Br}(K) \longrightarrow \bigoplus_v \text{Br}(K_v) \xrightarrow{\oplus \text{inv}_v} \mathbf{Q}/\mathbf{Z} \longrightarrow 0.$$

The lemma follows from the functoriality mentioned in Remark 5.6. \square

Lemma 5.9. Let $\mathbb{k}(J)$ be the function field of J . Suppose that $g \in \mathbb{k}(J)$ satisfies $\text{div}(g) = 2\tau_x^*(\Theta_J) - 2\Theta_J$ for some $x \in J[2]$. Then $g \circ [-1] = g$.

Proof. Note that $\text{div}([-1]^*(g)) = [-1]^*(2\tau_x^*(\Theta_J) - 2\Theta_J) = 2\tau_{-x}^*(\Theta_J) - 2\Theta_J = \text{div}(g)$ since $[-1]^*\Theta_J = \Theta_J$. Hence $[-1]^*g = cg$ for some constant c , and c has to be either 1 or -1 .

Let η be the generic point which corresponds to the divisor Θ_J . Write $\hat{\mathcal{O}}_\eta$ for the completion of the local ring \mathcal{O}_η (since Θ_J is an irreducible divisor, \mathcal{O}_η is a discrete valuation ring). Then there is an isomorphism

$$\hat{\mathcal{O}}_\eta \cong k(\Theta)[[t]],$$

where $k(\Theta)$ is the residue field of \mathcal{O}_η , and t is a uniformizer. Then $[-1]^* \in \text{Aut}(k(\Theta)[[t]])$ is induced by $[-1]$. Since $[-1]^*$ has order 2, $[-1]^*$ sends t to $(\pm t) + (\text{higher degree terms})$. By assumption, $v_\Theta(g) = -2$, where v_Θ denote the valuation along Θ_J . Hence if one views g as an element in $k(\Theta)((t))$, it is immediate that $[-1]^*g$ and g have the same leading term. Therefore $c = 1$, and this completes the proof. \square

Let J' be the Jacobian of another hyperelliptic curve and $\lambda : J \rightarrow J'$ be an isomorphism over \bar{K}_v . By functoriality, the isomorphism λ induces an isomorphism $\lambda^* : \mathcal{H}_{J',\Theta_{J'}} \rightarrow \mathcal{H}_{J,\Theta_J}$. It is easy to check that the map

$$\text{Isom}(J, J') \rightarrow \text{Isom}(\mathcal{H}_{J',\Theta_{J'}}, \mathcal{H}_{J,\Theta_J})$$

given by $\lambda \mapsto \lambda^*$ is a G_{K_v} -equivariant homomorphism. Now we show that the induced quadratic forms above are indeed the same for all quadratic twists. The following theorem generalizes [4, Lemma 5.2].

Theorem 5.10. *Suppose that $\chi \in \mathcal{C}(K_v)$. The canonical isomorphism $J[2] \cong J^\chi[2]$ identifies $\mathfrak{q}_{J,v}$ and $\mathfrak{q}_{J^\chi,v}$ for every place v .*

Proof. Fix an isomorphism $\lambda : J \rightarrow J^\chi$ defined over the field $\overline{K}_v^{\text{Ker}(\chi)}$. For every $\sigma \in G_{K_v}$, we have

$$\lambda^\sigma = \lambda \circ [\chi(\sigma)] = \lambda \circ [\pm 1].$$

Hence $(\lambda^*)^\sigma = (\lambda^\sigma)^* = [\pm 1]^* \circ \lambda^*$. For all g such that $\text{div}(g) = 2\tau_x^*(\Theta_J) - 2\Theta_J$ for some $x \in J[2]$, we have $[-1]^*g = g$ by Lemma 5.9. Therefore $(\lambda^*)^\sigma = \lambda^*$ for all $\sigma \in G_{K_v}$, whence $\mathfrak{q}_{J,v} = \mathfrak{q}_{J^\chi,v}$ since the following diagram commutes.

$$\begin{array}{ccccccc} 1 & \longrightarrow & \overline{K}_v^\times & \longrightarrow & \mathcal{H}_{J,\Theta_J} & \longrightarrow & J[2] \longrightarrow 0 \\ & & \parallel & & \uparrow \simeq \lambda^* & & \uparrow \simeq \\ 1 & \longrightarrow & \overline{K}_v^\times & \longrightarrow & \mathcal{H}_{J^\chi,\Theta_{J^\chi}} & \longrightarrow & J^\chi[2] \longrightarrow 0. \end{array}$$

□

Combining this theorem with [4, Theorem 3.9], we get the following.

Theorem 5.11. *Suppose that J is the Jacobian of a hyperelliptic curve C_f over a number field K . Suppose that $\chi \in \mathcal{C}(K)$. Then*

$$\dim_{\mathbf{F}_2} \text{Sel}_2(J/K) - \dim_{\mathbf{F}_2} \text{Sel}_2(J^\chi/K) \equiv \sum_v h_v(\chi_v) \pmod{2},$$

where χ_v is the restriction of χ to G_{K_v} and h_v is given in Definition 2.2.

6. 2-SELMER RANKS OF HYPERELLIPTIC CURVES

Let K be a number field and $f \in K[X]$ be a separable polynomial of odd degree (≥ 3) such that $\alpha_1, \alpha_2, \dots, \alpha_n$ are the roots of f . By an appropriate transformation of C_f , we may assume that α_i are algebraic integers. We are mainly interested in the case where $\text{Gal}(f) \cong S_n$ or A_n .

Let $\Delta_f := \prod_{i < j} (\alpha_i - \alpha_j)^2$ be the discriminant of the polynomial f . Let Σ be a set of primes containing all archimedean places, all primes above 2, and all primes that divide Δ_f (hence C_f , so $J(C_f)$ also, has good reduction at all primes not in Σ). We enlarge Σ so that $\text{Pic}(\mathcal{O}_{K,\Sigma}) = 1$, where $\mathcal{O}_{K,\Sigma}$ is the ring of Σ -integers, and fix it from now on. Note that

$$\begin{aligned} \sqrt{\Delta_f} &\in \mathcal{O}_{K,\Sigma}^\times \text{ if } \text{Gal}(f) = A_n, \text{ and} \\ \sqrt{\Delta_f} &\notin \mathcal{O}_{K,\Sigma}^\times \text{ if } \text{Gal}(f) = S_n. \end{aligned}$$

Lemma 6.1. (i) *If $\mathfrak{q} \in \mathcal{P}_i$ for some even i and $\chi_{\mathfrak{q}} \in \mathcal{C}(K_{\mathfrak{q}})$, then $\chi_{\mathfrak{q}}(\Delta_f) = 1$.*
(ii) *If $\mathfrak{q} \in \mathcal{P}_i$ for some odd i and $\chi_{\mathfrak{q}} \in \mathcal{C}(K_{\mathfrak{q}})$, then $\chi_{\mathfrak{q}}(\Delta_f) = 1$ if and only if $\chi_{\mathfrak{q}}$ is unramified.*

Proof. It is well-known that $\sqrt{\Delta_f}$ is fixed exactly by even permutations. The condition $\mathfrak{q} \in \mathcal{P}_i$ is equivalent to $\text{Frob}_{\mathfrak{q}}|_{K(J[2])} \in S_n$ being a product of $i+1$ disjoint cycles by Lemma 2.14. Therefore if i is even, then $\text{Frob}_{\mathfrak{q}}|_{K(J[2])}$ is an even permutation because n is odd, so $\sqrt{\Delta_f} \in K_{\mathfrak{q}}$. In other words, $\Delta_f \in (K_{\mathfrak{q}}^\times)^2$; i.e., $\chi_{\mathfrak{q}}(\Delta_f) = 1$ for all $\chi_{\mathfrak{q}} \in \mathcal{C}(K_{\mathfrak{q}})$. This shows (i). If i is odd, then $\text{Frob}_{\mathfrak{q}}|_{K(J[2])}$ is an odd permutation, so it does not fix $\sqrt{\Delta_f}$. Hence $\Delta_f \notin (K_{\mathfrak{q}}^\times)^2$. Therefore by

the definition of Σ and \mathcal{P}_i (not intersecting Σ), the discriminant Δ_f must generate $\mathcal{O}_{\mathfrak{q}}^{\times}/(\mathcal{O}_{\mathfrak{q}}^{\times})^2 \cong \mathbf{Z}/2\mathbf{Z}$, from which (ii) follows. \square

Lemma 6.2. *Define $\mathcal{A} \subset K^{\times}/(K^{\times})^2$ by*

$$\mathcal{A} := \ker(\mathcal{O}_{K,\Sigma}^{\times}/(\mathcal{O}_{K,\Sigma}^{\times})^2 \rightarrow \prod_{\mathfrak{q} \in \mathcal{P}_0} \mathcal{O}_{\mathfrak{q}}^{\times}/(\mathcal{O}_{\mathfrak{q}}^{\times})^2).$$

Then \mathcal{A} is generated by Δ_f if $\text{Gal}(f) \cong S_n$, and \mathcal{A} is trivial if $\text{Gal}(f) \cong A_n$.

Proof. If $\text{Gal}(f) \cong S_n$, there is only one intermediate field $K(\sqrt{\Delta_f})$ between K and $K(J[2])$ of degree 2 over K . Hence if $\alpha \in \mathcal{O}_{K,\Sigma}^{\times}/(\mathcal{O}_{K,\Sigma}^{\times})^2$ is not equal to Δ_f , then $K(\sqrt{\alpha})$ and $K(J[2])$ are linearly disjoint over K . Then by the Chebotarev Density Theorem, there exists a prime \mathfrak{q} and $\text{Frob}_{\mathfrak{q}} \in \text{Gal}(K(J[2])K(\sqrt{\alpha})/K)$ such that

- $\text{Frob}_{\mathfrak{q}}(\sqrt{\alpha}) = -\sqrt{\alpha}$, and
- $\text{Frob}_{\mathfrak{q}}|_{K(J[2])} \in \text{Gal}(f) = S_n$ is an n -cycle.

By Lemma 2.12 and the conditions on $\text{Frob}_{\mathfrak{q}}$, we have $\mathfrak{q} \in \mathcal{P}_0$ and $\sqrt{\alpha} \notin \mathcal{O}_{\mathfrak{q}}^{\times}$, so $\alpha \notin \mathcal{A}$. Lemma 6.1(i) with $i = 0$ shows that $\Delta_f \in \mathcal{A}$. If $\text{Gal}(f) \cong A_n$, the same argument with $\Delta_f \in (\mathcal{O}_{K,\Sigma}^{\times})^2$ shows that \mathcal{A} is trivial. \square

For a prime \mathfrak{q} , we write $\text{res}_{\mathfrak{q}}(\text{Sel}_2^{\mathfrak{q}}(J/K))$ for the image of $\text{Sel}_2^{\mathfrak{q}}(J/K)$ of the map

$$\text{res}_{\mathfrak{q}} : H^1(K, J[2]) \rightarrow H^1(K_{\mathfrak{q}}, J[2]).$$

Lemma 6.3. *The \mathbf{F}_2 -vector space $\text{res}_{\mathfrak{q}}(\text{Sel}_2^{\mathfrak{q}}(J/K))$ is a Lagrangian subspace in the metabolic space $(H^1(K_{\mathfrak{q}}, J[2]), q_{J,\mathfrak{q}})$, where $q_{J,\mathfrak{q}}$ is the quadratic form arising from the Heisenberg group of $J[2]$.*

Proof. By Lemma 3.8,

$$d_2(\text{res}_{\mathfrak{q}}(\text{Sel}_2^{\mathfrak{q}}(J/K))) = \frac{1}{2}d_2(H^1(K_{\mathfrak{q}}, J[2])).$$

Then [13, Proposition 4.9], [13, Corollary 4.7] and Lemma 5.8 show that $\text{res}_{\mathfrak{q}}(\text{Sel}_2^{\mathfrak{q}}(J/K))$ is a Lagrangian subspace. \square

Let \mathfrak{q} be a place where $\mathfrak{q} \nmid p\infty$ and J has good reduction. Recall that the localization map

$$\text{loc}_{\mathfrak{q}} : \text{Sel}_2(J/K) \rightarrow \alpha_{\mathfrak{q}}(1_{\mathfrak{q}}) \cong J[2]/(\text{Frob}_{\mathfrak{q}} - 1)J[2]$$

is given by evaluating cocycles at $\text{Frob}_{\mathfrak{q}}$. The following two Propositions are the main ingredient of Theorem 6.7.

Lemma 6.4. *Suppose that $\text{Gal}(f) \cong A_n$ or S_n . For an even number i , suppose that $\ell \in \mathcal{P}_i$ and $\psi_{\ell} \in \mathcal{C}(K_{\ell})$. Then, there is a $\chi \in \mathcal{C}(K)$ such that*

$$\text{Sel}_2(J^{\chi}/K) = \text{Sel}_2(J, \chi_{\ell}).$$

Proof. Recall that $\text{Pic}(\mathcal{O}_{K,\Sigma}) = 0$, so $\text{Pic}(\mathcal{O}_{K,\Sigma(\ell)}) = 0$. Thus global class field theory shows that

$$\mathcal{C}(K) = \text{Hom}(\mathbf{A}_K^{\times}/K^{\times}, \pm 1) = \text{Hom}((\prod_{v \in \Sigma(\ell)} K_v^{\times} \times \prod_{\mathfrak{q} \notin \Sigma(\ell)} \mathcal{O}_{\mathfrak{q}}^{\times})/\mathcal{O}_{K,\Sigma(\ell)}^{\times}, \pm 1).$$

Let

$$\begin{aligned} Q &:= \mathcal{P} - \{\mathcal{P}_0 \cup \Sigma(\ell)\}, \\ M &:= \mathcal{O}_{K, \Sigma(\ell)}^\times, \\ G &:= \prod_{\mathfrak{q} \in \mathcal{P}_0} \mathcal{O}_{\mathfrak{q}}^\times, \text{ and} \\ H &:= \prod_{\mathfrak{q} \in Q} \mathcal{O}_{\mathfrak{q}}^\times \times \prod_{v \in \Sigma(\ell)} K_v^\times. \end{aligned}$$

Define a map ϕ

$$\begin{aligned} \phi : \mathcal{C}(K) = \text{Hom}((G \times H)/M, \pm 1) &\longrightarrow \text{Hom}(H, \pm 1) \\ &\cong \prod_{\mathfrak{q} \in Q} \text{Hom}(\mathcal{O}_{\mathfrak{q}}^\times, \pm 1) \times \prod_{v \in \Sigma(\ell)} \text{Hom}(K_v^\times, \pm 1). \end{aligned}$$

Then by Lemma 6.2 and Lemma 4.8, ϕ is surjective if $\text{Gal}(f) \cong A_n$, and $\text{Im}(\phi)$ is exactly $\{g \in \text{Hom}(H, \pm 1) : g(\Delta_f) = 1\}$ if $\text{Gal}(f) \cong S_n$. In either case, for all local characters $\psi_\ell \in \mathcal{C}(K_\ell)$, there is a global character $\chi \in \mathcal{C}(K)$ such that

- $\chi_\ell = \psi_\ell$,
- $\chi_{\mathfrak{q}}|_{\mathcal{O}_{\mathfrak{q}}^\times} = 1_{\mathfrak{q}}$ for $q \in Q$,
- $\chi_v = 1_v$ for $v \in \Sigma$

by Lemma 6.1, where $\chi_\ell, \chi_{\mathfrak{q}}, \chi_v$ are the restrictions of χ to $G_{K_\ell}, G_{K_{\mathfrak{q}}}, G_{K_v}$, respectively. For example, if $\text{Gal}(f) \cong S_n$, the existence of such a χ can be seen by Lemma 6.1(i). Then by Lemma 2.15, $\alpha_{\mathfrak{p}}(1_{\mathfrak{p}}) = \alpha_{\mathfrak{p}}(\chi_{\mathfrak{p}})$ for all places \mathfrak{p} except ℓ . \square

Proposition 6.5. *Suppose that $\text{Gal}(f) \cong A_n$ or S_n and suppose that $d_2(\text{Sel}_2(J/K)) \geq 2$. Then there exist infinitely many $\chi \in \mathcal{C}(K)$ such that*

$$d_2(\text{Sel}_2(J^\chi/K)) = d_2(\text{Sel}_2(J/K)) - 2.$$

Proof. Decreasing 2-Selmer rank by 2 by twisting when $n = 3$ and $\text{Gal}(f) \cong A_3$ is done in [8, Proposition 5.2]. Thus, assume that C_f satisfies $(*)$ (Definition 3.3). Choose $\ell \in \mathcal{P}_2$ so that $d_2(\text{Im}(\text{loc}_\ell)) = 2$, which is possible by Lemma 3.4 and the Chebotarev Density Theorem. Then $d_2(\text{Sel}_{2,\ell}(J/K)) = d_2(\text{Sel}_2(J/K)) - 2$. By Lemma 3.8,

$$d_2(\text{Sel}_2^\ell(J/K)) = d_2(\text{Sel}_{2,\ell}(J/K)) + 2,$$

whence $\text{Sel}_2^\ell(J/K) = \text{Sel}_2(J/K)$. Taking any ramified character $\psi_\ell \in \mathcal{C}_{\text{ram}}(K_\ell)$, we see that $d_2(\text{Sel}_2(J, \psi_\ell)) = d_2(\text{Sel}_2(J/K)) - 2$. The rest follows from Lemma 6.4. \square

Proposition 6.6. *Suppose that $\text{Gal}(f) \cong A_n$ or S_n . Then there exist infinitely many $\chi \in \mathcal{C}(K)$ such that*

$$d_2(\text{Sel}_2(J^\chi/K)) = d_2(\text{Sel}_2(J/K)) + 2.$$

Proof. First assume that C_f satisfies $(*)$. Choose $\ell \in \mathcal{P}_2$ so that $\text{Im}(\text{loc}_\ell) = 0$ and $\text{Frob}_\ell|_{J(K[2])} \in \text{Gal}(f) \subseteq S_n$ is a product of 3 disjoint cycles of odd lengths. Choosing such an ℓ is possible by Lemma 3.4 and the Chebotarev Density Theorem. If $n = 3$ and $\text{Gal}(f) \cong A_3$, one can find a sufficiently big field N containing $K(J[2])$ that is Galois over K , and $c(\sigma) = 0$ for $\sigma \in G_N$ and $c \in \text{Sel}_2(J/K)$. Then there are infinitely many primes $\ell (\in \mathcal{P}_2)$ such that $\text{Frob}_\ell|_{\text{Gal}(N/K)} = 1$ by the Chebotarev density theorem.

In either case, we have $\text{Sel}_2(J/K) = \text{Sel}_{2,\ell}(J/K)$. By Lemma 3.8 and Lemma 6.3.

$$d_2(\text{Sel}_2^\ell(J/K)) = d_2(\text{Sel}_{2,\ell}(J/K)) + 2$$

and $\text{res}_\ell(\text{Sel}_2^\ell(J/K))$ is a Lagrangian subspace (Lemma 6.3) of the metabolic space $(H^1(K_\ell, J[2]), q_{J,\ell})$ that intersects $\alpha_\ell(1_\ell)$ trivially. Let $\mathcal{C}_{\text{ram}}(K_\ell) = \{\psi_1, \psi_2\}$. Then $\alpha_\ell(1_\ell) \cap \alpha_\ell(\psi_1) = \alpha_\ell(1_\ell) \cap \alpha_\ell(\psi_2) = \{0\}$ by Lemma 2.16, and $\alpha_\ell(\psi_1) \cap \alpha_\ell(\psi_2) = \{0\}$ by Lemma 4.7. By Lemma 5.2, there are exactly 2 Lagrangian subspaces that intersect $\alpha_\ell(1_\ell)$ trivially, so there exists a $\psi_\ell \in \mathcal{C}_{\text{ram}}(K_\ell)$ such that $\alpha_\ell(\psi_\ell) = \text{res}_\ell(\text{Sel}_2^\ell(J/K))$. Hence it follows that $d_2(\text{Sel}_2(J, \psi_\ell)) = d_2(\text{Sel}_2(J/K)) + 2$. Now Lemma 6.4 proves the proposition. \square

Finally, Proposition 6.5 and Proposition 6.6 show the following by induction.

Theorem 6.7. *Suppose that C_f is a hyperelliptic curve over a number field K such that $\text{Gal}(f) \cong A_n$ or S_n . Let J denote the Jacobian of C_f . Then for all $r \equiv d_2(\text{Sel}_2(J/K)) \pmod{2}$, there exist infinitely many quadratic characters $\chi \in \mathcal{C}(K)$ such that $d_2(\text{Sel}_2(J^\chi/K)) = r$.*

7. PARITY OF 2-SELMER RANKS OF JACOBIANS OF HYPERELLIPTIC CURVES

We continue to assume that J is the Jacobian of C_f , where $n = \deg(f)$ is odd.

Definition 7.1. For every $v \in \Sigma$ and $\chi_v \in \mathcal{C}(K_v)$, we define $\omega_v : \mathcal{C}(K_v) \rightarrow \{\pm 1\}$ by

$$\omega_v(\chi_v) := (-1)^{h_v(\chi_v)} \chi_v(\Delta_f).$$

Define

$$\delta_v := \frac{1}{|\mathcal{C}(K_v)|} \sum_{\chi \in \mathcal{C}(K_v)} \omega_v(\chi) \quad \text{and} \quad \delta := (-1)^{d_2(\text{Sel}_2(J/K))} \prod_{v \in \Sigma} \delta_v.$$

Definition 7.2. Define a function $\mathcal{C}(K) \rightarrow \mathbf{Z}_{>0}$ by

$$\|\chi\| := \max\{\mathbf{N}(\mathfrak{q}) : \chi \text{ is ramified at } \mathfrak{q}\},$$

where $\mathbf{N}(\mathfrak{q})$ is the index of the residue field of $K_{\mathfrak{q}}$. If $X > 0$, let $\mathcal{C}(K, X) \subset \mathcal{C}(K)$ be the subgroup

$$\mathcal{C}(K, X) := \{\chi \in \mathcal{C}(K) : \|\chi\| < X\}.$$

The following proposition is in fact the same as [4, Proposition 7.2] in a slightly more general setting (hyperelliptic curves). For $\chi \in \mathcal{C}(K)$, let

$$r(\chi) := d_2(\text{Sel}_2(J^\chi/K))$$

and χ_v be the restriction of χ to G_{K_v} .

Proposition 7.3. *Suppose that $\chi \in \mathcal{C}(K)$. Then*

$$r(\chi) \equiv r(1_K) \pmod{2} \iff \prod_{v \in \Sigma} \omega_v(\chi_v) = 1.$$

Proof. Let θ be a (formal) product of primes not in Σ such that χ is ramified exactly at the primes which divide θ . Then by Lemma 6.1,

$$\prod_{\mathfrak{q} \notin \Sigma} \chi_{\mathfrak{q}}(\Delta_f) = (-1)^{|\{\mathfrak{q} : \mathfrak{q} \in \mathcal{P}_i \text{ for odd } i \text{ and } \mathfrak{q} | \theta\}|}.$$

Note that for $\mathfrak{q}|\theta$, we have $(-1)^{h_{\mathfrak{q}}(\chi_{\mathfrak{q}})} = \chi_{\mathfrak{q}}(\Delta_f)$ by Lemma 2.16, Lemma 6.1, and Remark 4.4. Therefore Theorem 5.11 and Lemma 2.15 show that

$$\begin{aligned} r(\chi) \equiv r(1_K) \pmod{2} &\iff (-1)^{\sum_v h_v(\chi_v)} = 1 \\ &\iff \prod_{v \in \Sigma} \omega_v(\chi_v) \chi_v(\Delta_f) \prod_{v \notin \Sigma} \chi_v(\Delta_f) = 1. \end{aligned}$$

Clearly $\prod_v \chi_v(\Delta_f) = 1$, so this completes the proof. \square

The following theorem is remarkable theorem due to Klagsbrun, Mazur, and Rubin ([4, Theorem 7.6]) (for the elliptic curve case).

Theorem 7.4. *For all sufficiently large X ,*

$$\frac{|\{\chi \in \mathcal{C}(K, X) : d_2(\text{Sel}_2(J^X/K)) \text{ is even}\}|}{|\mathcal{C}(K, X)|} = \frac{1 + \delta}{2}.$$

Proof. See the proof of Theorem 7.6 in [4]. Without difficulty, one can see [4, Theorem 7.6] can be extended to the hyperelliptic curve case. \square

Proposition 7.5. *Suppose that K has a real embedding $K \hookrightarrow K_{v_0}$. Then*

$$\delta_{v_0} = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{4} \\ 0 & \text{if } n \equiv 3 \pmod{4}. \end{cases}$$

Proof. Let η be the sign character in $\mathcal{C}(K_{v_0}) = \text{Hom}(K_{v_0}^\times, \pm 1)$ sending negative numbers to -1 . Suppose that f has $2k_1 - 1$ real roots and $2k_2$ complex roots so that $2k_1 + 2k_2 - 1 = n$. Let $\beta_1, \beta_1, \beta_2, \beta_2, \dots, \beta_{k_2}, \beta_{k_2}$ denote the complex roots of f , where β_i is the complex conjugate of β_i . Then by an appropriate rearrangement of the roots, we get

$$\Delta_f = \prod_{i < j} (\alpha_i - \alpha_j)^2 = c\bar{c} \prod_{1 \leq i \leq k_2} (\beta_i - \bar{\beta}_i)^2$$

for some c . Hence $\eta(\Delta_f) = (-1)^{k_2}$. By Lemma 2.20, we deduce that

$$(-1)^{h_{v_0}(\eta)} = (-1)^{k_1 - 1}.$$

Therefore $\delta_{v_0} = 1/2(1 + \omega_{v_0}(\eta)) = 1/2(1 + (-1)^{k_1 + k_2 - 1})$, so the proposition follows from the equality $2k_1 + 2k_2 - 1 = n$. \square

As an easy application, we have

Corollary 7.6. *Suppose that $n \equiv 3 \pmod{4}$, and K has a real embedding. Then for all sufficiently large X , we have*

$$|\{\chi \in \mathcal{C}(K, X) : r(\chi) \text{ is even}\}| = |\{\chi \in \mathcal{C}(K, X) : r(\chi) \text{ is odd}\}| = \frac{|\mathcal{C}(K, X)|}{2}.$$

Remark 7.7. If $n \equiv 1 \pmod{4}$ or if K has no real embedding, we have to know values of δ_v other than δ_{v_0} to compute an accurate density. In fact, the “disparity constant” δ may not be zero. We display an example in next section.

Theorem 6.7 and Theorem 7.4 show the following.

Theorem 7.8. *Suppose that C_f is a hyperelliptic curve defined over a number field K such that $n = \deg(f)$ is odd. Suppose that $\text{Gal}(f) \cong S_n$ or A_n , and the disparity constant δ is neither -1 nor 1 . Then for every $r \geq 0$, the Jacobian J of C_f has infinitely many quadratic twists J^X such that $d_2(\text{Sel}_2(J^X/K)) = r$.*

Corollary 7.9. *Suppose that C_f is a hyperelliptic curve defined over a number field K . Let $n = \deg(f)$, and suppose that $n \equiv 3 \pmod{4}$ and $\text{Gal}(f) \cong S_n$ or A_n . Suppose further that K has a real embedding. Then for every $r \geq 0$, the Jacobian J of C_f has infinitely many quadratic twists J^χ such that $d_2(\text{Sel}_2(J^\chi/K)) = r$.*

8. EXAMPLES

In this section, we give an explicit example of a hyperelliptic curve C_h/\mathbf{Q} such that $d_2(\text{Sel}_2(J^\chi/\mathbf{Q}))$ has constant parity for all quadratic twists J^χ (J := the Jacobian of C_h), so it defies (2) in the introduction. More precisely, the main result of this section is the following.

Proposition 8.1. *Suppose that C_h is a hyperelliptic curve over \mathbf{Q} whose affine model is*

$$y^2 = h(x) := -273(6x+1)(91x^2+54x+9)(100x^2+60x+1)$$

Let J denote the Jacobian of C_h . Then $d_2(\text{Sel}_2(J^\chi/\mathbf{Q}))$ is even for all quadratic twists J^χ of J .

Let E_f be an elliptic curve labelled 1440D1 in [1]:

$$y^2 = f(x) := x^3 - 273x + 1672.$$

Then

$$E_f[2] = \{\infty, (-19, 0), (8, 0), (11, 0)\}.$$

Define an isomorphism $\psi : E_f[2] \rightarrow E_f[2]$ by sending $(\alpha_i, 0)$ to $(\beta_i, 0)$, where

$$\alpha_1 = -19, \alpha_2 = 8, \alpha_3 = 11, \beta_1 = 8, \beta_2 = 11, \text{ and } \beta_3 = -19.$$

Clearly, ψ does not come from an isomorphism $E_f \rightarrow E_f$ since E_f does not have complex multiplication (the j -invariant of E_f is not an integer).

Proposition 4 in [3] shows that the Jacobian of the curve defined by $y^2 = h(x)$ where

$$h(x) = -(-810Ax^2 + 81B)(81Ax^2 - 90B)(-90Ax^2 - 810B)$$

is isomorphic to the quotient of $E_f \times E_f$ by the graph of ψ . The constant A and B are as in Proposition 4 in [3], and one can see $A = 1990170 = -B$ by simple algebra. Then by a rational transformation of $y^2 = h(x)$ by

$$x = \frac{3x' + 1}{x'}, y = \frac{cy'}{x'^3},$$

where $c = 2^2 \times 3^{14} \times 5^2 \times 7 \times 13$, we get

$$y'^2 = -273(6x' + 1)(91x'^2 + 54x' + 9)(100x'^2 + 60x' + 1).$$

By abuse of notation, let

$$h(x) := -273(6x + 1)(91x^2 + 54x + 9)(100x^2 + 60x + 1).$$

Then the above observation shows that J is isogenous to $E_f \times E_f$ over \mathbf{Q} .

Definition 8.2. Let A be an abelian variety over a number field K . Define

$$\text{Sel}_n(A/K) := \{x \in H^1(K, A[n]) : \text{res}_v(x) \in \text{Im}(i_v) \text{ for all places } v\},$$

where res_v is the restriction map

$$\text{res}_v : H^1(K, A[n]) \rightarrow H^1(K_v, A[n])$$

and i_v is the Kummer map $i_v : A(K_v)/nA(K_v) \rightarrow H^1(K_v, A[n])$. If p is a prime, we define $\text{Sel}_{p^\infty}(A/K)$ to be the direct limit of the Selmer groups $\text{Sel}_{p^k}(A/K)$.

Lemma 8.3. *Suppose that C_h and E_f are as above. Then for any $\chi \in \mathcal{C}(\mathbf{Q})$,*

$$d_2(\text{Sel}_2(J^\chi/\mathbf{Q})) \equiv d_2(J(\mathbf{Q})[2]) \pmod{2}$$

Proof. Since J and $E_f \times E_f$ are isogenous over \mathbf{Q} , the induced map

$$\text{Sel}_{2^\infty}(J/\mathbf{Q}) \rightarrow \text{Sel}_{2^\infty}((E_f \times E_f)/\mathbf{Q})$$

has finite kernel and cokernel. Hence

$$\text{corank}_{\mathbf{Z}_2}(J/\mathbf{Q}) = \text{corank}_{\mathbf{Z}_2}((E_f \times E_f)/\mathbf{Q}),$$

so $\text{corank}_{\mathbf{Z}_2}(J/\mathbf{Q})$ is even. In a similar way, one can see that $\text{corank}_{\mathbf{Z}_2}(J^\chi/\mathbf{Q})$ is even for all quadratic twists J^χ . We have the following two exact sequences:

$$0 \rightarrow J(\mathbf{Q}) \otimes \mathbf{Q}_2/\mathbf{Z}_2 \rightarrow \text{Sel}_{2^\infty}(J/\mathbf{Q}) \rightarrow \text{III}[2^\infty] \rightarrow 0, \text{ and}$$

$$0 \rightarrow J(\mathbf{Q})/2J(\mathbf{Q}) \rightarrow \text{Sel}_2(J/\mathbf{Q}) \rightarrow \text{III}[2] \rightarrow 0,$$

where the group III is the Shafarevich-Tate group of J/\mathbf{Q} . From the above exact sequences, we see that

$$\begin{aligned} d_2(\text{Sel}_2(J/\mathbf{Q})) &= \text{rk}(J(\mathbf{Q})) + d_2(J(\mathbf{Q})[2]) + d_2(\text{III}_{\text{div}}[2]) + d_2(\text{III}/\text{III}_{\text{div}}[2]) \\ &= \text{corank}_{\mathbf{Z}_2}(J/\mathbf{Q}) + d_2(\text{III}/\text{III}_{\text{div}}[2]) + d_2(J(\mathbf{Q})[2]) \\ &\equiv d_2(J(\mathbf{Q})[2]) \pmod{2}, \end{aligned}$$

where the last congruence holds by the following. Note that C_h has a rational point ∞ , so the $(K$ -rational) theta divisor given by $j : C_h \rightarrow J$ sending P to $[P - \infty]$ produces a principal polarization. See Section A.8.2 of [2] for more details. Then the congruence follows from the following two general facts.

- (i) If A is an abelian variety over a number field K that has a principal polarization coming from a K -rational (Weil) divisor, then there is a pairing

$$\text{III}_{A/K} \times \text{III}_{A/K} \rightarrow \mathbf{Q}/\mathbf{Z},$$

that is alternating and nondegenerate after division by maximal divisible subgroup.

- (ii) If there is a finite abelian group B with an alternating non-degenerate pairing

$$B \times B \rightarrow \mathbf{Q}/\mathbf{Z},$$

then $d_2(B[2])$ is even.

Similarly, one can see

$$\dim_{\mathbf{F}_2}(\text{Sel}_2(J^\chi/\mathbf{Q})) \equiv \dim_{\mathbf{F}_2}(J^\chi(\mathbf{Q})[2]) \pmod{2}$$

for all quadratic twists J^χ . Then the lemma follows from Proposition 1.7. \square

Proof of Proposition 8.1. It is easy to see $d_2(J(\mathbf{Q})[2]) = 2$ by Lemma 2.12. Then Lemma 8.3 completes the proof. \square

We show one more example in the following proposition.

Proposition 8.4. *Let $J(C_g)$ be the Jacobian of hyperelliptic curve C_g given by*

$$y^2 = g(x) = (2x+1)(3x^2+4x+2)(3x^2+2x+1).$$

Then $d_2(\text{Sel}_2(J(C_g)^\chi/\mathbf{Q}))$ is even for all $\chi \in \mathcal{C}(K)$.

Proof. Let E' be the elliptic curve $y^2 = x^3 - x$. Let

$$\alpha_1 = 1, \alpha_2 = -1, \alpha_3 = 0, \beta_1 = -1, \beta_2 = 0, \text{ and } \beta_3 = 1.$$

Then one can proceed exactly in the same way as above to get a hyperelliptic curve $C_{g'}$ given by $y^2 = g'(x)$ for some $g' \in \mathbf{Q}[X]$, whose Jacobian is isogenous to $E' \times E'$ and is a quadratic twist of $J(C_g)$. It is easy to see $d_2(J(C_g)(\mathbf{Q})[2]) = 2$ by Lemma 2.12. Then the rest follows from Lemma 8.3. \square

ACKNOWLEDGEMENTS

The author is very grateful to his advisor Karl Rubin for sharing his deep ideas and insight into the subject. Also the author wants to thank to Bjorn Poonen, and Heng Su for providing a simpler proof of Lemma 5.9, and for programming used in the discovery of the example in Proposition 8.1. He extends his thanks to the referees for previous and current versions of this article for helpful suggestions, as well as to Chan-Ho Kim and Wan Lee for comments. He is also grateful to Dennis Eichhorn for proofreading.

REFERENCES

- [1] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, 1992.
- [2] M. Hindry and J. H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.
- [3] E. W. Howe, F. Leprévost, and B. Poonen. Large torsion subgroups of split Jacobians of curves of genus two or three. *Forum Math.*, 12(3):315–364, 2000.
- [4] Z. Klagsbrun, B. Mazur, and K. Rubin. Disparity in Selmer ranks of quadratic twists of elliptic curves. *Ann. of Math. (2)*, 178(1):287–320, 2013.
- [5] K. Kramer. Arithmetic of elliptic curves upon quadratic extension. *Trans. Amer. Math. Soc.*, 264(1):121–135, 1981.
- [6] B. Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.*, 18:183–266, 1972.
- [7] B. Mazur and K. Rubin. Finding large Selmer rank via an arithmetic theory of local constants. *Ann. of Math. (2)*, 166(2):579–612, 2007.
- [8] B. Mazur and K. Rubin. Ranks of twists of elliptic curves and Hilbert’s tenth problem. *Invent. Math.*, 181(3):541–575, 2010.
- [9] W. G. McCallum. Tate duality and wild ramification. *Math. Ann.*, 288(4):553–558, 1990.
- [10] J. S. Milne. *Arithmetic duality theorems*, volume 1 of *Perspectives in Mathematics*. Academic Press, Inc., Boston, MA, 1986.
- [11] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.
- [12] T. Oda. The first de Rham cohomology group and Dieudonné modules. *Ann. Sci. École Norm. Sup. (4)*, 2:63–135, 1969.
- [13] B. Poonen and E. Rains. Random maximal isotropic subspaces and Selmer groups. *J. Amer. Math. Soc.*, 25(1):245–269, 2012.
- [14] K. Rubin. *Euler systems*, volume 147 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2000. Hermann Weyl Lectures. The Institute for Advanced Study.
- [15] E. F. Schaefer. Computing a Selmer group of a Jacobian using functions on the curve. *Math. Ann.*, 310(3):447–471, 1998.
- [16] J.-P. Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2002. Translated from the French by Patrick Ion and revised by the author.
- [17] C. Towse. Weierstrass points on cyclic covers of the projective line. *Trans. Amer. Math. Soc.*, 348(8):3355–3378, 1996.

DEPARTMENT OF MATHEMATICS, UC IRVINE, IRVINE, CA 92697, USA

E-mail address: `myungjuy@math.uci.edu`